A -= Spaghetti Phreaker's =- Production

CDP 's

Spaghetti Phreakers Cookbook

The definitive guide to Italian Phreaking

Aggiornamento by Aken

Versione 2.0 15/10/1998

DISCLAIMER:

Tutte le notizie contenute in questa guida sono da considerarsi a puro scopo informativo. L'autore, CDP, non si assume alcuna responsabilità per l'uso che ne farete.

Informare non è in alcun modo illegale.

Potete distribuire gratuitamente questa guida attraverso qualsiasi canale purchè ne lasciate intatto il contenuto. Se trovate qualcuno che si è appropriato indebitamente del contenuto, o di solo una parte di esso, della guida riferitecelo al nostro indirizzo e-mail.

Contenuti:

A -= Spaghetti Phreaker's =- Production

CDP 's

Spaghetti

Phreakers

Cookbook

The definitive guide to Italian Phreaking

Aggiornamento by Aken

Versione 2.0 15/10/1998

DISCLAIMER:

Tutte le notizie contenute in questa guida sono da considerarsi a puro scopo informativo. L'autore, CDP, non si assume alcuna responsabilità per l'uso che ne farete.

Informare non è in alcun modo illegale.

Potete distribuire gratuitamente questa guida attraverso qualsiasi canale purchè ne lasciate intatto il contenuto. Se trovate qualcuno che si è appropriato indebitamente del contenuto, o di solo una parte di esso, della guida riferitecelo al nostro indirizzo e-mail.

Contenuti:

1.3 Panorama attuale

Sezione 2: Le Cabine Telecom

2.1 Introduzione

2.2 I Rotor

2.3 Il grande sogno della ricarica

2.4 Metodi per chiamare gratis

2.5 Cosa fare con il telefono

2.6 Balle spaziali

Sezione 3: Utenza domestica e Internet

3.1 Introduzione

3.2 Le centrali Telecom

3.3 Internet Gratuita

3.4 Trasferimento di chiamata

3.5 Telefono col lucchetto

3.6 La magica blue box

3.7 Vampirare i cordless

3.8 Calling Cards

3.9 Giocare via modem gratis

Sezione 4: Telefonia cellulare

4.1 Introduzione

4.2 Cellulari e clonazioni ETACS

4.3 La SIM card

4.4 Centro ricariche TIM

4.5 Trucchi vari

4.6 Codici segreti di cellulari GSM

Sezione 5: Storia e varie

5.1 Non solo scatole blu

5.2 La Natura giuridica del Phone Phreaking

5.3 Mentor’s last words

5.4 Lo sfogo di un phreaker

Appendice 1: Leggende metropolitane.

Sezione 1: Introduzione al CookBook

1.1 Introduzione

di CDP

Durante i primi mesi di vita del progetto di Spaghetti Phreakers, da più parti mi era giunta la richiesta di fare in modo che tutte le info contenute nel sito potessero essere scaricate in un colpo solo e lette comodamente off-line, qualcuno mi chiedeva addirittura di scrivere una guida che racchiudesse tutto ciò che al momento si sapeva e si poteva fare. Era buffo per me constatare che quanto mi si chiedeva era quello che io stesso andavo cercando sulla rete, ed in effetti mi è sembrato giusto prendere la stessa decisione che presi quando decisi di iniziare con Spaghetti Phreakers: se davvero non esiste niente del genere, bisogna farlo.

Ecco allora cosa vuole essere questa guida: il riassunto di quello che abbiamo raccolto fino ad ora col progetto di Spaghetti Phreakers, col vostro aiuto e la vostra collaborazione.

Chiunque pensa di sapere qualcosa di più di quanto scritto su questa guida, è pregato di contattarmi, al mio email: spaghettiphreak@hotmail.com.

Le nuove info saranno subito sul sito e sulle successive release di questa guida, che comunque non sarà rilasciata su basi regolari ma solo quando il nuovo materiale sarà sufficiente a giustificare l'operazione.

CDP (alias Spaghettiphreak)

1.2 Upgrader

di Etern0

In questi anni di confusione sul mondo del Phreaking, questa guida porta alla luce la vera essenza di questa antica arte. (^_^) Validissime informazioni provenienti dai maggiori esponenti che il panorama attuale offre, lavori di gruppo, informazioni tecniche ufficiali e tantissime altri ingegni.

Okkio perché questo CoockBook è in constante aggiornamento e disponibile nel web di Spaghetti

Phreakers.

Etern0 (CoockBook Upgrader)

3. Il Panorama Attuale

di CDP

Bisogna dire che questo non è decisamente un periodo d'oro per il phreaking, che qui in Italia ha visto la sua golden Age nei primi anni 90, quando per sbafare le telefonate c'era solo l'imbarazzo della scelta, ora l'unico fenomeno eclatante sembra la comparsa dei famosi 'green' per la connessione ad Internet

Adesso la Telecom ha affiliato le unghie e l'antica arte del Phreaking rischia di scomparire.

Si intravede una luce nella liberalizzazione del settore delle telecomunicazioni, ma resta ancora tutto da vedere. I bug delle cabine vengono corretti man mano che vengono scoperti e così al phreaker non resta altro che la vandalica soluzione di portarsi a casa un rotor per souvenir, per poi scoprire che non è capace ad interfacciarlo al PC. Ma ragazzi, noi siamo tanti e siamo furbi! Se ci impegnamo possiamo scoprire sempre nuove vie! Per cui uniamoci e rimbocchiamoci le maniche. Spaghetti Phreakers è lì per questo.

Per contattare Spaghetti Phreakers:

e-mail: spaghettiphreak@hotmail.com

internet: http://come.to/spaghettiphreakers

http://members.xoom.com/spaghettiphr/

Hanno collaborato in vari modi alla riuscita (?) di Spaghetti Phreakers (rigorosamente in ordine sparso): Etern0, Timescape, Blum, Chatrobot, Turi Turi, Fab, DarkSoul, Vespasian, ellegi, Master of Puppets, Master, Scanman, McCrack, Space Navigator, Telecomico, Savio, Chaos Engine e tanti altri che ora non ricordo…

Sezione 2: Le Cabine Telecom

2.1 Introduzione

di CDP

Le cabine telecom sono state per me il primo obiettivo quando decisi di avvicinarmi al Phreaking: riuscire a non pagare il mitico gettone era un obiettivo raggiunto poche volte ma sempre con estrema soddisfazione.

Degli articoli tuttora presenti su Spaghetti Phreakers abbiamo deciso di tenerne fuori parecchie perché non più praticabili (alcune a rileggerle col senno di poi non lo sono mai state), mentre ne abbiamo messe alcune che forse rimangono praticabili in qualche sperduta parte d'Italia.

2.2 I Rotor ovvero i telefoni arancioni di mamma Telecom

Quattro articoli sul funzionamento e lo smontaggio di questi simpatici apparecchietti.

2.2.1 I Rotor, questi sconosciuti

di Master of Puppets

Allora, ora vi spiego cosa so io dei rotor: I fili che arrivano al rotor sono 4, e non 2 come si potrebbe supporre: due sono per la voce, gli altri sono per lo scambio dati del telefono

con la sua centrale. (se ti connetti ai due fili voce con una beige box (lineman handset) il

telefono rileva tale operazione, e la linea viene bloccata.). Il rotor è alimentato dall'esterno, dalla tensione di rete.

La carcassa è spessa almeno 3 mm, in acciaio, e, se lo apri (a

martellate è un pò dura, viene bene col piede di porco se il telefono

non è tanto nuovo, ovvero se hai un pò di spazio per operare. Personalmente ne ho visto uno fatto fuori a picconate, ma credo sia un poco indecente)dentro trovi un' altra gabbia che isola il telefono vero e proprio.

tiri la gabbia verso l'esterno e apri le due cerniere ai lati, ora hai in mano un rotor vero e proprio.

Che altro non è che un cilindro con tante fessure, in ognuna delle quali cade una monetina.

(puoi quindi capire che i soldi che ficchi nel telefono lì rimangono fino a quando non finisci la conversazione, o, per essere più precisi, quando il tempo della tua conversazione finisce.)

(capirai anche che, essendo finito il numero di slots, finito è il tempo di una conversazione, anche se ci sbatti dentro solo 500 lire).

Il riconoscimento delle monetine avviene tramite differenti parametri:

peso, dimensioni, e, il più cattivo di tutti, materiale.

(quindi le 50 lire con il nastro isolante non le puoi più usare, nemmeno le monetine di ghiaccio (le ho viste), e neppure le monetine passate sotto il tram.

La moneta col filo? inabilitata dalla presenza stessa del rotore e da una lama a ghigliottina che chiude la fessura delle monetine e non ti permette di estrarre la tua truccata.).

Ora, che fare? L'unica è aprire il bastardo, e trovare, all'interno della gabbia, poco sopra il cilindro, uno switch con il quale aggiungere il credito, come nei videogiochi.

(credo comunque che il telefono sia allarmato, in Inghilterra lo sono, quindi sfasciarlo con un brutal assault potrebbe essere comunque pericoloso). Questo e più o meno il riassuntino di ciò che so sui rotor, per quanto riguarda il telefono.

Il lettore di tessere è un altro capolavoro di ingegeria: tre testine di lettura e due di cancellazione situate nella parte posteriore dell'apparato, la tessera (è flessibile, hai notato?) viene mossa da nastri, e la sua posizione è controllata da fotoaccoppiatori (praticamente non li puoi fottere).

2. Smontare un Rotor

di ellegi e Vespasian

Allora innanzitutto volevo premettere Ke tutto questo e' Konsiderato molto illegale, poiKe' oltre a essere un furto a mamma Telekom e' anke vandalismo quindi un due o tre anni (forse) di galera non te li toglie nessuno :))

Per smontare facilmente un rotor dovresti averne gia uno Kon tutta la Karcassa... (non tentare di aprirlo Kon piedi di porKo perKe' e' faticoso...) quindi sradiKandolo dalla sua sede... poi avendo la Karcassa potrai facilmente riprodurre la kiave che potrai costruire con

un tondino d'ottone, andando a tentativi se sei un po bravo con la limetta... Credimi, e' stato gia fatto... Non l'ho fatto personalmente ma l'ho visto con i miei okki!!!

Basta una pinza per segger (o come cazzo si scrive) che riempia bene i buchi di quelle strane viti sulfondo (immagino :)) e se vi serve un lettore di tessere allora non dovete

fare altro che allargare la distanza tra il coperchio del rotor e quello dell'aggiuntivo con un piede di porco o simili e cercare di agganciare la levetta interna con un gancetto molto sottile, infilandolo nella fessura che lascia libero il passaggio....

3. Guida all’assalto dei Rotor

di Master of Puppets

Allora, premetto il fatto che non credo all'approccio "morbido" con il rotor. I perchè sono tanti, ma, alla base, stà il fatto che:

non si può. Non c'è tempo.

Con questo non voglio contraddire chi ha fatto tutti i suoi bravi esperimenti di assalto

morbido, ma, di questi, vorrei sapere quanti ne sono riusciti.

Un assalto morbido presuppone una conoscenza della macchina approfondita,

cosa, che grazie alla censura operata da Mamma Telecom su tutte le cose che la

riguardano, purtroppo non abbiamo; allora perchè non farcela, una conoscenza?

Altra cosa: sapete che comunque un brutal assault è un atto di vandalismo di quelli

pesanti (ma va'?), e quindi, se volete farlo, non fatevi sgamare, perchè i pulotti, per

leggenda tramandata, non capiscono il linguaggio dei phreakers.

Osservate il telefono

Il telefono, come ho già detto, è un piccolo gioiello di ingegneria, ed è stato studiato

per resistere agli attacchi più violenti: non ha buchi o fessure dove inserire attrezzi,

e que pochi che ha (fessura per le monete, pozzetto del resto) sono fatti in modo da

impedire comunque l'accesso alle parti importanti del telefono.

Il lettore, anche lui, è realizzato nello stesso modo, e, nutrite poche speranze di

fargli male con poco.

Da dove cominciamo?

Allora, il punto da cui cominciare, mi pare, deve essere un telefono, no?

Abbandoniamo il tono scherzoso, perchè non serve.

Sceglietevi un telefono isolato, se non nella vostra zona, nella zona affianco, o nel

paese affianco; ma assolutamente sceglietevene uno dove la gente non passi ogni

tre per due.

Scieglietevi la vostra vittima con la cabina, non con quell' assurda conchiglia di plexiglas intorno, il perchè è facilmente intuibile.

Se decidete di attaccare fatelo di notte, non da soli nè in 32 persone. Ricordatevi che il rischio di farvi sgamare è direttamente proporzionale con il numero delle persone.

Andiamo

Se la cabina ha ancora la luce accesa rompetela.

Non è difficile: coprite con del nastro adesivo la lastra di plexiglas, poi colpite con forza con un martello (dalla parte delle code, che entra più facilmente nella lastra) il nastro adesivo non permette che le scheggie cadano a terra o in testa a voi.

Per assorbire il rumore, se ce ne è bisogno, usate uno straccio tra la mazza e la lastra.

Il buio vi aiuterà a passare inosservati.

La serratura del rotor: vi siete mai chiesti perchè è semi conica?

Ha quella forma per dirottare colpi ad essa indirizzati.

Fate una prova: puntate uno scalpello (anche senza la lama va bene, anzi, meglio, che non vi scassate se vi scappa) alla sua base e date una botta con il vostro fidato martello.

Se il colpo che date è abbastanza forte vi rimane in mano l'anello conico che copre la serratura vera e propria.

Bel souvenir, ma capirete quanto è inutile attaccare da qui.

Devo stringere, se no mi dilungo troppo in particolari di cui non vi interessa affatto.

Puntate al fianco della serratura, tra la parte Grigia e quella arancione, e colpite, in direzione verso l' esterno.

Potranno essere necessari più colpi, avvolgete il martello nello straccio per

assorbire i rumori da fabbro, e allargate il coperchio.

inserite il vostro piede di porco e fate forza. Il bastardo dovrebbe aprirsi tranquillamente.

Tirate fuori la gabbia (vedi articolo precedente) e fate quello che volete.

Tips

Non è necessario fare tutto in una volta.

Potete organizzare il tutto in notti successive, per diluire il rischio di farvi fottere.

Fatto il danno, filate, non si sa mai. Potrete tornare con comodo il giorno dopo, e, senza attrezzi, investigare in santa pace, facendovi passare, in caso di sgamo, per uno appena entrato per telefonare che ha trovato il telefono distrutto.

Il lettore di tessere è ancorato dall' interno del telefono, quindi per portarvelo via senza danneggiarlo dovete scardinare il telefono.

Se non badate al risultato, agite con violenza e usando un cuneo (tipo quando spaccate la legna) infilato dall' alto, sradicatelo dal corpo principale.

E' un modo un pò rozzo, lo ammetto, di dare assalto a una cabina, e non lo potrete ripeteremolto spesso, ma, per esperienza personale, funziona molto meglio di altre cose.

Bye bye, e viaggiage con gli occhi aperti.

4. Info tecniche sui rotor

di Avatar666 (dal suo Personal CoockBook)

Prima di tutto bisogna fare una distinzione tra il '"Terminale telefonico pubblico ROTOR O.V.

c/antieffrazione" (cabina a gettoni o a gettoni + schede) ed il "Terminale telefonico pubblico T.P.D.C. / R.I.

c/modulo LIOD / R.I." (cabina solo a schede). Nota: i dati qui scritti sono stati copiati dai manuali ORIGINALI, quindi prendetelo per oro colato, perché E' TUTTO VERO. Ho aggiunto, poi, del e mie semplici, ma "terribili", considerazioni che si possono fare osservando queste tabelle che scriverò dopo ogni tabella introdotte da

"N.B.:".

Rotor O.V.

Alimentazione:

telealimentato

Tensione di linea:

102V max

Corrente di linea costante:

Gancio ON 30 mA; Gancio OFF 24 mA

Connessione alla linea O.V:

"a" e "b"

Programmazione valore incasso:

remoto

Tutti i criteri di gestione telefonia (Selezione, gestiti dal livello 3 del protocollo HDLC in criteri di incasso, ecc.):

tecnica Overvoice

Dimensioni monete gestite dal terminale:

Diametro: min. 16.5mm; max 32mm.

Spessore: min. Non limiti; max 2.8mm

Capacità di accumolo:

20 pezzi

Capacità cassetta raccogli monete:

1000 ±2000 pezzi

Selezionatore monete:

di tipo elettronico con capacità di

discriminare 6 conii controllando diametro,

lega e spessore

Avviso fonico di fine credito:

20" prima della disconnessione

Avviso ottico di fine credito:

20" prima della disconnessione

Display:

Lcd 16 cifre

Tipo di lettore gestito dal terminale:

lettore integrato O.D./R.I.

Dimensioni:

440 x 240 x 185mm versione normale

705 x 240 x 185mm versione corazzata

Peso:

Kg. 16.100 versione normale

Kg. 32.200 versione corazzata

N.B.:

o La programmazione del valore d'incasso è remota, caxxo;

o Controlla la lega delle monete... Argh!.

o E' in grado di "discriminare 6 conii". Me ne manca 1! Infatti:

1. 50 lire

2. 100 lire

3. 200 lire

4. 500 lire

5. Gettone telefonico

-E poi?- (Non credo sia la moneta segreta di 007...)

T.P.D.C.

Alimentazione:

telealimentato

Tensione di linea:

102V max

Corrente di linea costante:

Gancio ON 30 mA; Gancio OFF 24 mA

Connessione alla linea O.V:

"a" e "b"

Programmazione valore incasso:

remoto

Tutti i criteri di gestione telefonia (Selezione, gestiti dal livello 3 del protocollo HDLC in criteri di incasso, ecc.):

tecnica Overvoice

Tipo di carte gestite dal terminale:

Carta telefonica, Credito telefonico, Credito

commerciale

Avviso fonico di fine credito:

20" prima della disconnessione

Avviso ottico di fine credito:

20" prima della disconnessione

Display:

Lcd alfanumerico, 20 caratteri per 2 righe

Dimensioni:

315 x 245 x 230mm

Peso:

14,7 kg.

N.B.:

o La programmazione del valore d'incasso è anche qua remota, riCaxxo.

2. I codici di errore delle cabine Telecom

di Avatar666 (dal suo Personal CoockBook)

Quante volte ti sarà capitato di leggere in una cabina guasta (e non) uno strano

codice? Beh ora puoi sapere cosa vuol dire...

Codici di errore del ROTOR O.V. (Cabina a monete, per intenderci!)

E100 Errore del validatore

E101 Errore della tastiera

E102 Errore Display

E103 Cassetta piena

E104 Possibile guasto trasmettitore microtelefono

E105 Preallarme Cassetta Piena

E106 Errore Ram del Micro

E107 Incaglio di una scheda

E200 Errore foto ingresso tasca (sempre buio)

E201 Errore foto uscita tasca

E202 Errore foto ingresso tasca (sempre in luce)

E203 Errore Saracinesca introduzione

E204 Errore foto canaletta incasso

E205 Errore Saracinesca incasso/restituzione

E206 Errore foto Magnete incasso/restituzione

E300-E301-E302-E303 Anomalia al meccanismo di movimentazione rotore

E304 Incaglio canale di incasso

E305 Sezione di credito F.S.

E306 Sezione di debito F.S.

E305-E306 F.S. totale L.I.

E305-E306-E107 Mancanza canale di Con. APP. L.I.

E307 Da 1 a 7 tasche in Fuori Servizio

E400 Guasto al magnete di incasso/restituzione

E401 Assenza colloquio con translatore (manca livello 2)

E402 Errore dati configurazione (RAM ESTERNA)

E403 Interruzione breve in conversazione con riconfigurazione del terminale

E404 Sportello aperto

E405 Ostruzione nella bocchetta restituzione, sul display a gancio a riposo

compare: F.S.

con la bocchetta introduzione moneta chiusa.

E406-E407 Asportazione cassetta, ed apertura sportello cassaforte

E500 Guasto RAM ESTERNA

E501 30 sganci consecutivi senza conteggio

E502-E503 Errore foto introduzione durante l'introduzione/validazione

E504 8 o più tasche in Fuori Servizio

E505 Errore di ricezione della configurazione del sistema

E506 Manca alimentazione alla linea (ac-bc)

E507 Mancanza colloquio tra base micro e interfaccia linea O.V.

Codici di errore del T.P.D.C. / R.I. (Cabina a schede, per intenderci!)

E10 Sportello aperto

E11 Errore tastiera

E12 Errore display

E13 Errore trasmettitore microtelefono

E14 Mancanza colloquio con sistema di centrale

E15 Mancanza alimentazione di linea

E16 Assenza colloquio interfaccia di linea

E17 RAM del μP guasta

E20 Sezione credito F.S.

E21 Sezione debito F.S.

E22 Scheda incagliata

E23 Lettore F.S.

E24 Assenza colloquio con il lettore

E25 Tentativo di frode lettore in conv. a carte telefoniche (!)

E26 Dati errati da sistema

E27 Dati errati RAM esterna

E30 Contatori errati

E31 Guasto RAM esterna

E32 Guasto EEPROM

E33 Riconfigurazione

L.I. Lettore integrato

F.S. Fuori Servizio

O.V. OverVoice

3. Procedura di test dei rotor

di Avatar666 (dal sua Personal CoockBook)

La "Procedura di test" consente di fare molte cose interessanti (leggetevele), soprattutto di ricavare informazioni "utili", ma prima bisogna aprire la cabina (non vi consiglio di usare metodi "violenti" (piede di porco, ecc.),la cosa migliore sarebbe copiare la chiave o farne una nuova, perché è importante che NON SI NOTI il vostro intervento, e modificare la posizione degli switch a fianco del Display.

ROTOR O.V.

Posizionare il microswitch SW1 in modo OFF ed il microswitch SW2 in modo ON, dare un comando di RESET, sul display verrà visualizzato il numero della release a sinistra e la data di emissione a destra (identificazione release). Bravo, sei in "Test mode"! Ecco i test che si possono fare: TEST 1 - FONIA, SONERIA, BIP RICEVITORE, BOLLINI

Digitare 1 sulla tastiera, sul display compare 01 lampeggiante a sinistra. In questa fase 01 si possono effettuare 4 test diversi:

1 - TEST FONIA: Pigiando 1 dalla tastiera. Serve per verificare la fonia nel microtelefono

2 - TEST SONERIA: Pigiando 2 dalla tastiera. Serve per verificare il circuito soneria (se

montata)

3 - TEST BIP RICEVITORE: Pigiando 3 dalla tastiera. Serve per verificare il bip di fine

credito nel ricevitore

4 - TEST BOLLINI: Pigiando 4 della tastiera. Serve per verificare il numero totale dei bollini presenti nell'apparecchio che saranno così visualizzati:

I.L. 0.0 00/00/00 = identifica la Release della MIL

e subito dopo

04 P xx = che indica bollini presenti (xx)

Se il numero risulta meno di 12, è possibile individuare i bollini non connessi:

Pigiando 5 della tastiera vengono visualizzati in ordine progressivo i bollini presenti riscontrati che saranno così visualizzati:

05 C1 B1-B7 = C1 indica il primo cavetto collegato alla Plug µP della MIL (in basso) e B1öB7 i bollini riscontrati.

Subito dopo viene visualizzato:

05 C2 B1-B5 = C2 indica il secondo cavetto collegato alla Plug µP della MIL (in alto) e B1-B5 i bollini riscontrati.

Nel caso di mancata connessione di uno o più bollini, il numero relativo al bollino non verrà visualizzato.

L'identificazione dei bollini non visualizzati si ottiene contando i connettori in ordine progressivo del cavetto di appartenenza (C1 o C2) partendo dalla connessione sulla Plug µP della MIL che non viene conteggiato fino al numero del bollino non visualizzato.

I bollini sono connessi nel seguente ordine:

Connettore C1 (in basso)

Connettore C2 (in alto)

B1 = MIL/O.V. 4 KV

B1 = Selezionatore

B2 = Microtelefono

B2 = Piastra Meccanismi

B3 = Sportello Rotor

B3 = Plug Cell/O.V.

B4 = Batteria

B4 = Mod. Elettr. Base

B5 = Cassaforte

B5 = Ram Backup

B6 = Rotor O.V. BE

B7 = Modulo LIOD/RI

Al termine sul Display verrà visualizzato 01 lampeggiante. Per uscire dai test citati premere un qualunque tasto e sul Display ricompare 01 lampeggiante. Per uscire dal test 01 lampeggiante digitare un numero che non sia 1-2-3-4 sul display 01-EO.

TEST 2 - RAM MICRO

Digitare "2" e verificare la comparsa sul display della scritta 02-EO.

TEST 3 - RAM ESTERNA

Digitare "3" e verificare la scritta 03-EO.

TEST 4 - TEST VISUALIZZAZIONE CONTATORI

Digitare "4" sul display verranno evidenziati in sequenza i contenuti dei contatori gestionali e tecnici suddistinti per tipo (sulla destra del display), e la quantità (sulla sinistra del display) espresse da numeri max di 4 cifre che nel seguito saranno indicati con xxxx; cioè:

xxxx -200 = numero gettoni incassati (evidenziato co "-200" in quanto attualmente il gettone costa 200 lire)

xxxx 100 = numero pezzi 100 lire incassati

xxxx 200 = numero pezzi 200 lire incassati

xxxx 500 = numero pezzi 500 lire incassati

E le seguenti informazioni accessorie:

xxxx - 0 = NIL numero comandi di incasso ricevuti dall'apparecchio

xxxx - 1 = NGE numero gettoni equivalenti incassati

xxxx - 2 = numero pezzi accettati dal validatore

xxxx - 3 = numero pezzi scartati dal validatore

xxxx - 4 = NICD nunero comandi di incasso ricevuti dall'apparecchio per conversazioni a

carta di Debito

xxxx - 5 = NRCD numero di unità riscontrate per conversazioni a carta di Debito

xxxx - 6 = NICC numero comandi di incasso ricevuti dall'apparecchio per conversazioni a

carta di credito

L.200 = Costo del gettone

TEST 5 - TEST DISPLAY

Digitare "5" e verificare sul display la comparsa di tutti i numeri in tutte le posizioni da "9" a "1" a al termine verificare la scritta 05 EO

TEST 6 - TEST MOTORE ED ENCODER ASSOLUTO

Digitare "6" e verificare la scritta 06 EO

TEST 7 - TEST DINAMICO-FUNZIONALE DI TUTTI GLI ATTUATORI ELETTROMECCANICI EDEI

SENSORI DELL'APPARECCHIO

Digitare "7" e verificare la scritta 07 EO

TEST 8 - VISUALIZZAZIONE SEQUENZIALE DEI CODICI DI ERRORE

Digitare "8": se successivamente all'ultimo RESET dell'apparecchio non vi è stato un errore che abbia determinato un F.S., eventuali codici diagnostici presenti nello storico vengono visualizzati in modo automatico (Visualizzazione storico dei codici di errore). Se vi è stato un F.S.: anche se autoripristinato sul display viene visualizzata una sequenza formata da tutti i codici diagnostici presenti nello storico più

il codice di errore che ha determinato il F.S. dell'apparecchio. Più volte l'apparecchio è andato in F.S. più sequenze saranno visualizzate. Le sequenze hanno un codice progressivo che compare a sinistra del display mentre a destra saranno visualizzati uno per volta i codici di errore inerenti a quella sequenza. L'avanzamento dei codici/sequenza avviene manualmente digitando un qualsiasi tasto della tastiera. A fine sequenze eventuali codici diagnostici presenti nello storico vengono visualizzati in modo automatico. La visualizzazione sequenziale dei codici di errore può essere ripetuta indefinitivamente senza uscire dallo stato di test, all'uscita da quest'ultimo sia con RESET che per time out di 40 sec. di inattività, si azzera la memoria dei codici e avviene soltanto se tali sono stati visualizzati almeno una volta. In generale l'uscita da qualsiasi test per reset o per time out, che non abbia interessato il test 8, non determina l'azzeramento della memoria dello storico sequenziale dei codici degli errori.

TEST 9 - RESET DEL LETTORE INSTALLATO

Digitare "9" e verificare la scritta 09 EO. Questo test consente di ripristinare una eventuale perdita di configurazione del lettore installato.

TEST 10 - VERIFICA INTERRUTTORE SPORTELLO

Digitare "0" sul display comparirà 10 e subito dopo lo stato dell'interruttore relativo allo sportello e cioè: S A (sportello aperto)

S C (sportello chiuso)

Per verificare il buon funzionamento dell'interruttore bisogna controllare la coerenza che sul display ad apparecchio aperto risulti S A, e ad apparecchio chiuso risulti S C. Digitando un qualsiasi tasto si esce dal test.

TEST 11 - VERIFICA CHIUSURA/APERTURA BOCCHETTA INTRODUZIONE MONETE

Digitare "*" sul display comparirà 11 in modo lampeggiante. Si potrà eseguire l'apertura o la chiusura della bocchetta nel modo seguente:

A. Digitando il tasto "1" sul display comparirà "11 01" e la bocchetta verrà comandata in chiusura.

B. Digitando il tasto "2" sul display comparirà "11 02" e la bocchetta verrà comandata in apertura.

Le suddette indicazioni sul display rimangono per circa 3 secondi per poi ritornare con la visualizzazione di

"11" per dare la possibilità di fare una nuova scelta. L'uscita dal test avviene per T.O. di 40 secondi o digitando un qualsiasi altro tasto non utilizzato dal test.

Se durante l'effettuazione della procedura di test fossero riscontrate delle anomalie esse saranno evidenziate con il relativo codice di errore. Se il test è tutto OK l'apparecchio è pronto per entrare in servizio; pertanto si riportano i microcontatti secondo la configurazione OFF - OFF.

T.P.D.C.

Posizionare l'unico microswitch verso l'alto.

Dare un comando di RESET al pulsante posto vicino al microswitch. Sul display viene visualizzato:
STATO DI TEST

REL. nn.nn xx/xx/xx

(REL.....: identificazione release)

TEST 1: FONIA - SONERIA - BIP RICEVITORE - BOLLINI

Digitare 1 sulla tastiera di selezione, sul display compare TEST 01 lampeggiante. In questa fase TEST 01

lampeggiante si possono effettuare 4 test diversi e cioè:

1 - TEST FONIA: Confermare "1", sul display viene visualizzato TEST FONIA; verificare la fonia nel microtelefono che rimane attiva per circa 1 min. dopo di che viene visualizzato in seconda riga FINE TEST a conferma della chiusura del test fonia e subito dopo ricompare TEST 01 lampeggiante.

2 - TEST SONERIA: Digitare "2", sul display viene visualizzato TEST SONERIA; verificare, se è montata la soneria elettronica, che suoni; dopo circa 20 sec. viene visualizzato il seconda riga FINE TEST con la ricomparsa sul display di TEST 01 lampeggiante.

3 - TEST BEEP RICEVITORE: Digitare "3", sul display viene visualizzato TEST BEEP RICEVITORE; verificare il beep di avviso fine credito nel ricevitore che rimane attivo in modo intermittente per circa 20 sec.

dopo di che viene visualizzato in seconda riga FINE TEST con la ricomparsa sul display di TEST 01

lampeggiante.

TEST 2: INTERFACCIA DI LINEA

Digitare "2" e verificare sul display la comparsa del messaggio TEST 02 I. LINEA seguito da EO in seconda riga.

TEST 3: PIASTRA LOGICA

Digitare "3" e verificare sul display la comparsa del messaggio TEST 03 P. LOGICA seguita da EO in seconda riga.

TEST 4: VISUALIZZAZIONE CONTATORI

Digitare "4" sul display compare TEST 04 CONTATORI e subito dopo verranno evidenziati in sequenza i contenuti dei contatori suddistinti per tipo (sulla sinistra del display), e la quantità (sulla destra) espresse da numeri di max. 4 cifre che nel seguito saranno indicati con "xxxx" cioè:

CONT NICD xxxx = numeri incassi carta telefonica

CONT NRCD xxxx = numeri riscontri carta telefonica

CONT NICC xxxx = numeri incassi carta di credito

VALORE SCATTO 200 = costo del gettone

Al termine, sul display in seconda riga comparirà il messaggio FINE TEST.

TEST 5: DISPLAY

Digitare "5" e verificare sul display la scritta TEST 05 DISPLAY e subito dopo la comparsa di tutti i numeri su due righe da 0 a 9; al termine comparirà in seconda riga il messaggio FINE TEST.

TEST 6: MOTORE - ATTUATORE SARACINESCA

Digitare "6" e verificare sia la movimentazione del tamburo che quella della saracinesca. Sul display TEST

06 MEC. LET. e subito dopo LETTORE INTEGRATO e al termine in seconda riga FINE TEST.

TEST 7: LETTURA DELLE SCHEDE - BUZZER - LED

Digitare "7". Sul display compare il messaggio LETTORE INEGRATO e subito dopo INSERIRE UNA CARTA; introdurre una carta telefonica non esaurita; la carta sarà trattenuta e poi restituita; sul display comparirà il messaggio CARTA TELEFONICA e subito dopo RITIRARE LA CARTA; si attiverà il buzzer per alcuni istanti. Passare una carta di credito; sul display comparirà CREDITO TELEFONICO se la carta è Telecom, CREDITO COMMERCIALE se commerciale, per poi ritornare sul display INSERIRE UNA CARTA.

L'uscita da questo test avviene o digitando un tasto della tastiera o per time-out di 40 sec., visualizzando il messaggio FINE TEST in seconda riga.

NOTA: Una carta telefonica con valore viene restituita dalla bocchetta superiore, mentre una carta telefonica azzerata viene restituita dalla bocchetta inferiore.

TEST 8: VISUALIZZAZIONE SEQUENZIALE DEI CODICI DI ERRORE

Digitare "8". Se successivamente all'ultimo TEST 8 visualizzato non vi è stato un errore che abbia determinato un F.S., eventuali codici diagnostici presenti nello storico vengono visualizzati sul display come di seguito:

In prima riga: ERRORI STORICI

In seconda riga: E11 oppure E12, ecc.

Se vi è stato un F.S. anche se autoripristinante sul display viene visualizzata una sequenza formata dal codice di errore che ha determinato il F.S. più eventuali codici diagnostici presenti nello storico. Più

volte l'apparecchio è andato in F.S. più sequenze saranno visualizzate come di seguito:

In prima riga: SEQUENZA N.01

In seconda riga: CODICE E10 oppure Exx

L'avanzamento dei codici/sequenza avviene manualmente digitando un qualsiasi tasto della tastiera. A fine sequenze gli eventuali codici diagnostici presenti nello storico vengono visualizzati come descritto nella prima parte ma in modo automatico. Successivamente sul display vengono visualizzati in modo automatico i contatori statistici relativi al lettore integrato, distinti per tipo (sulla sinistra), e per quantità (sulla destra) espresse da numeri max di 4 cifre che nel seguito saranno indicati con "xxxx" e cioè: In prima riga: CONTATORI LETTORE

In seconda riga: CONT FRODE GON xxxx: contatore frode gancio ON

CONT FRODE GOFF xxxx: contatore frode gancio OFF

CONT ERR LETT2 xxxx: contatore errore lettura T2

CONT INCAGLIO xxxx: contatore incaglio scheda

CONT CANCEL OK xxxx: contatore scheda OK

CONT CANCEL KO xxxx: contatore scheda KO

Termina con TEST 08 SEQUENZE e in seconda riga FINE TEST. Questo test può essere ripetuto

indefinitivamente senza uscire dallo stato di test. All'uscita da quest'ultimo sia per reset che per time-out di 40 sec. di inattività, viene azzerata la memoria dello storico sequenziale dei codici di errore, mentre i contatori statistici relativi al lettore integrato vengono azzerati solo superando la soglia di 9999. L'uscita da qualsiasi test per reset o per time-out che non abbia interessato il TEST 8, non determina l'azzeramento della memoria dello storico sequenziale dei codici degli errori.

TEST 9: RESET DEL LETTORE INTEGRATO

Digitare "9". Sul display comparirà TEST 09 RESET LET.

Subito dopo viene visualizzato:

In prima riga: LETTORE INTEGRATO

In seconda riga: REL nn.nn gg/mm/aa

(REL..... = identificazione della release software)

Subito dopo sul display comparirà FINE TEST.

Questo test consente di mandare un reset al lettore integrato.

TEST 10: VERIFICA INTERRUTTORE SPORTELLO

Digitare "0". Sul display comparirà TEST 10 SPORTELLO e subito dopo in seconda riga lo stato dell'interruttore relativo allo sportello e cioè:

SPORTELLO APERTO

SPORTELLO CHIUSO

Per verificare il buon funzionamento dell'interruttore bisogna controllare la coerenza tra il messaggio sul display e lo stato dello sportello. Per uscire dal test premere un tasto qualsiasi; sul display in seconda riga comparirà il messaggio FINE TEST.

TEST 11: INDICE DEI CODICI DI ERRORE

Digitare "*". Sul display comparirà TEST 11 INDICE. In modo automatico e/o manuale pigiando un tasto saranno visualizzati in ordine crescente tutti i codici di errore in seconda riga, con la relativa descrizione sulla prima riga.

TEST 12: AZZERAMENTO CONTATORI

Digitare "#". Sul display comparirà TEST 12 AZZ.CONT. lampeggiante. Se si vogliono azzerare i contatori bisogna confermare l'operazione digitando nuovamente il tasto "#". Premendo un qualsiasi altro tasto si esce dal test senza azzerare i contatori. Sul display in seconda riga comparirà FINE TEST.

FINE TEST

Se durante l'effettuazione della procedura di test fossero riscontrate delle anomalie esse saranno evidenziate con il relativo codice di errore. Se l'esito del test è positivo, l'apparecchio è pronto per entrare in servizio; pertanto si riporta il microswitch verso il basso (normale funzionamento) e si preme nuovamente il pulsante di reset.

3. **Il grande sogno della ricarica/duplicazione delle schede Telecom**

Tutto era iniziato per me con l'MTF project, apparso su BFI ma avuto da me in anteprima circa 10 giorni prima. Sembrava possibile così ricaricare le schede telefoniche prepagate telecom, ma poi ci arrivò una bella doccia fredda… grazie all'amico Timescape che ci ha evitato di sprecare altro tempo: le schede infatti risultavano copiabilissime: basta avere la testina di un Rotor, e registrare la benda magnetica di una scheda carica su un nastro abbastanza doppio, e incollare questo su una scheda vuota. Il problema era che le schede così ottenute risultavano TROPPO identiche fra loro…

Rimane una strada da percorrere: riuscire a sgamare l'algoritmo di generazione delle schede telecom in modo da produrne anziche copiare quelle esistenti. Così bisognerà sì aspettare che le schede vengano attivate dalla telecom, ma almeno le si potrà consumare prima degli sventurati clienti…

2.3.1 Brutte Notizie per le ricariche

di Timescape

Era un pezzo che volevo scrivere quanto segue, ma non ho mai trovato il tempo e la voglia; questo e'

quanto.

A riguardo della duplicazione delle tessere magnetiche prepagate telecom (quelle da 5.000/10.000 per le cabine, tanto per intenderci) :

la duplicazione pura e', oltre che non facile, perfettamente inutile... da circa tre anni tutte le cabine in Italia sono collegate a quella che si chiama rete intelligente (la stessa che gestisce i numeri verdi, i 166/144, etc.), che non e' altro il collegare un bel database generical purpose ad una rete telefonica pubblica. L'unico dato che viene utilizzato delle tessere

magnetiche e' il numero di serie (impresso nella prima parte della banda magnetica), il restante segnale (i soldi rimasti) anche se viene ancora modificato NON viene piu' assolutamente utilizzato. Su un database di gestione ad ogni numero di serie di card e' associato l'ammontare rimasto.

Per verificarlo prova banale: copiate una carta prepagata (almeno quello a questo punto dovreste saperlo fare), usate una delle due copie in una cabina e scendete ad esempio da 4000 a 3000lire di credito rimasto.

Provate l'altra copia in un'altra cabina e vedrete che vi dara' 3000lire rimaste e non 4000 sebbene quella tessera non sia stata toccata... scendete da 3000 a 2000 con questa seconda e riprovatele entrambe dove volete e le troverete scese a 2000lire... unica soluzione e' scoprire l'algoritmo dei numeri di serie (e penso sia banale, se non addirittura progressivo) e cambiare il numero di serie sulle carte copiate (complicato, bisogna sapere oltre che il bias del nastro magnetico anche la modulazione esatta usata da telecom,anzi dalla urmet, e riprodurla)...

per la cronaca per copiare la carta e' stato usato del nastro dei vecchi registratori a bobina (ancora usati in qualche rara sala d'incisione)...

2. L’Ormai defunto MTF Project

di Mc Crack

Tutto e' iniziato qualche mese fa, quando ad una delle tante fiere dell'informatica, mi capito' sotto il naso uno stranissimo oggetto.. all'apparenza sembrava un normalissimo gioco per bambini, di quelli tipo sapientino che ti insegnano il nome degli animali o come si dice in inglese "cesso".. era un gioco abbastanza vecchio e demente, infilando delle tessere nell'apposita fenditura ascoltavi una voce che spiegava cosa dovevi fare... dopo qualche secondo di osservazione notai pero' un particolare molto interessante: quelle tessere avevano il messaggio memorizzato su una banda magnetica molto simile a quella presente sulle carte telefoniche telecom. Per 10 mila valeva la pena di provare se questa malsana idea, infilare una carta telecom in un gioco per bambini, potesse avere un senso.. e cosi' comprai quel gioco.. In quel preciso momento prese il via il Progetto MTF... ovvero Magnetic Telecom Fuck..

Il Dimmy (prodotto dalla CABEL) ribattezzato MTF1 (per dargli un tono piu' serio) sembra davvero pensato per leggere le carte telefoniche.. la sua testina, oltre ad essere di buona qualita', e' fissata in modo da scorrere verso l'alto e verso il basso, in modo da centrare

esattamente la traccia magnetica presente sulla scheda.. Cosi', dopo aver collegato l'uscita dell'altoparlante all'ingresso della Sound Blaster, sono riuscito a memorizzarmi in formato wave la forma d'onda di diverse carte telefoniche.. e in questo articolo vi esporro' i risultati delle mie ricerche..

- Analisi dell'onda di una generica carta Telecom

Premessa: purtroppo la mia conoscenza dell'elettronica e' molto scarsa.. visto che ho pure frequentato il liceo scientifico, le poche informazioni che possiedo sono dovute a un puro interesse hobbystico.. i dati riportati qui di seguito sono dunque

piu' frutto dell'intuito che di una specifica preparazione.. percio' se vi dicono di mettere la mano sul fuoco per qualcosa che e' scritto qui sopra... non lo fate...
Studiando i wave di diverse carte da 10000 e 5000 mi sono accorto innanzi tutto che una scheda telecom e' sempre divisa in tre parti.
Le prime due sono fisse, ovvero tutte le volte che la carta viene usata non cambiano (fra la prima e la seconda serie c'e' sempre un impulso singolo)..
Con molta probabilita' dunque queste due parti contengono il numero di serie della tessera e la sua data di scadenza.. oltre ad altre informazioni specifiche della telecom. Poi c'e' la terza parte, e qui le cose si fanno piu' interessanti.. Infatti e' costituita da una strana sequenza di onde tutte uguali (se si esclude l'ultima).. mi sono dunque chiesto cosa dovrebbero rappresentare tutte queste onde messe in fila e, alla fine, mi sono reso conto che il loro numero corrisponde esattamente alle 200 lire rimaste sulla tessera.. ovvero una scheda nuova da 10000 ne avra' 50 e una da 5000, 25.. tutte le volte che usiamo la carta vengono
cancellate un numero di onde pari agli scatti effettuati e, ovviamente, l'assenza di queste onde significa che la vostra scheda e' scarica..
Ma andiamo un po' piu' in profondita'.. Innanzi tutto: quale tipo di memorizzazione e' usata ?
Qui il discorso si fa abbastanza incasinato.. da quello che ho letto esistono una caterva di modi di memorizzare dati su nastri magnetici, ognuno con i suoi standard e cazzi vari..
poi io non sono assolutamente preparato in questo settore e i mezzi di cui dispongo come avrete capito sono ridicoli.. pero' osservando bene i file in mio possesso sono arrivato ad alcune conclusioni.. innanzi tutto si tratta di un codice digitale, ovvero di una sequenza di 0 e

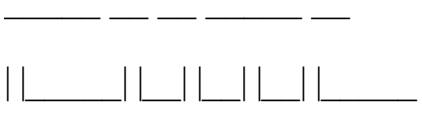
1. Infatti se si osserva il wave ingrandito, si nota che sono due tipi di onde che si ripetono in successione, cosa che implica necessariamente la presenza di due livelli logici..

Mi sono chiesto perche' le onde abbiano una forma cosi' strana, con quella rientranza come se fossero mozzate.. non sono sicuro, ma penso che sia dovuto al fatto che la testina magnetica ha una banda di lettura troppo stretta e perde parte delle informazioni memorizzate sulla traccia..

Si puo' ipotizzare come sarebbero dovute essere queste onde e ci si rende conto di un particolare importante: una e' costituita da un'unica oscillazione mentre l'altra ne ha due..

ovvero una ha la frequenza doppia dell'altra. E' una mia ipotesi ma questo si dovrebbe chiamare standard f-2f, che e' spesso utilizzato in carte di credito e carte bancarie..

Lo standard F2F e' molto intuitivo:



0 0 1 1 0 1 0

Come vedete se in un intervallo di tempo c'e' una sola oscillazione si tratta di uno zero e due se e' un uno..

La parte finale delle carte telecom, quella dove sono memorizzati i soldi, e' costituita da

una serie di zero terminata da un 1, mentre le prime due sono una sequenza di 1 e 0 variabile da tessera a tessera... e questa e' la sintesi di quello che sono riuscito a sapere dall'analisi dei wave..

- Cosa possiamo ottenere da queste informazioni -

E' possibile ricaricare una carta telecom ? A questo punto direi proprio di si..

vediamo in che modi...

(Tralascio di citare metodi come appoggiare la carta sullo schermo di un vecchio televisore, o immergerla in un forte campo magnetico... sono entrambe delle panzane galattiche...)

1: La ricopiatura analogica

Il primo metodo e' il piu' intuitivo: copiare l'onda di una scheda carica su una scarica..

Questo e' possibile perche' dai miei studi risulta che il nastro magnetico delle tessere e' riscrivibile (tanto riscrivibile che durante le mie prove ho mandato a puttane una scheda carica con 9400... spero che sia un investimento...)

Dunque si puo' usare il wave memorizzato dal Dimmy, assieme al circuito di un vecchio registratore, per pilotare dall'uscita della Sound Blaster una testina magnetica che copi sulla traccia della tessera scarica quello letto in precedenza da una carica..

Quali sono i problemi ? Il primo problema e' la larghezza della banda di lettura/scrittura della testina.. come infatti vi avevo fatto notare in precedenza, le onde memorizzate nel wave sono tagliate in alto e in basso.. un difetto che non e' rilevante se si vuole capire cosa c'e' scritto sulla tessera, ma che diventa fondamentale quando noi andiamo a scrivere questa onda parziale su una tessera scarica... il risultato e' che le cabine telefoniche rifiuteranno sdegnate la vostra carta..

Il problema puo' essere risolto comprando una testina delle giuste dimensioni.. e qui ci sono altri problemi: quali sono le giuste dimensioni, esistono testine di questo tipo

? ..Non ne ho

la minima idea..

Un altro problema fondamentale e' la velocita' di lettura/scrittura della tessera..

Il formato F2F impone una velocita' assolutamente costante della tessera, altrimenti si possono leggere degli 0 al posto degli 1 e viceversa.. poi se la velocita' e' troppo bassa si rischia di avere un segnale a bassa frequenza che viene tagliato dai filtri passa-alto della Sound Blaster.. rendendo vani i nostri sforzi.. consiglio di trovare un modo di leggere e scrivere la scheda con una velocita' di 4-5 cm/s ottenendo cosi' un segnale sui 150 Hz..

Nel caso dell'MTF1 (Dimmy) ho risolto il problema aumentando il voltaggio del motorino che fa avanzare la scheda, ottenendo un wave che corrisponde a una velocita' di lettura di circa

4,3 cm/s...

2: Sintesi digitale del segnale

Invece di ricopiare un segnale, con tutte le distorsioni connesse, si puo' usare un programma che ricrei un codice F2F del tutto identico a quello presente su una tessera..

Questo programma dovrebbe pilotare una piccola interfaccia attaccata alla porta parallela che inverte la polarita' della testina in modo da ricreare esattamente il codice di una carta carica... In questo modo oltre a essere piu' sicuri che la carta caricata funzioni si potrebbero inserire in una tessera molti piu' soldi del consentito..

la banda magnetica di una scheda non e' mai sfruttata fino in fondo, c'e' sempre un pezzo vuoto..

se si riempie quel pezzo prolungando la terza parte del codice si ottiene un scheda da 15000 e forse anche da 20000 (sempre che la telecom non abbia predisposto

delle protezioni in questo senso...).

I problemi di questo metodo sono i seguenti: in primo luogo non sono neanche sicuro che lo schema adottato sia l'F2F.. poi c'e' sempre il problema di reperire una testina magnetica larga quanto basta.. infine bisognerebbe calibrare il programma sulla giusta frequenza per far combaciare gli 0 e 1 di tessere originali e copiate..

Concludo dicendo che in questo momento sono impegnato nello studio di un sistema di ricarica seguendo le idee del primo metodo.. se mai dovesse funzionare aspettatevi un articolo con tutti i dati tecnici necessari per riprodurlo...

MTF UPDATE - 1

In attesa di progredire nella ricopiatura ho fatto qualche esperimento sulla possibilita' di rendere indelebili le tessere telecom... in modo ovviamente da riutilizzarle a piacere.

Non so se lo sapete, ma fino a non molto tempo fa era possibile fare una cosa di questo tipo piazzando nel punto giusto un piccolo pezzo di nastro adesivo. In questo modo il debole

campo magnetico utilizzato per aggiornare la scheda non riusciva a fare piu' il suo dovere, trasformado la tessera in una fonte inesauribile di gioia per il suo proprietario :))

Ora.. che si puo' fare adesso ? Devo dire che tutti i miei sforzi in questo senso sono stati vani.. ho provato praticamente tutto, da piccoli strati di isolante a bagni in liquidi adesivi. Ho ricoperto le tessere pure con la lacca per i capelli di mia nonna e gli ho fatto fare un bagno nell'acido ferrico (cosa inutile ma divertente). Infine, sapendo che le microonde provocano degli archi voltaici all'interno dei metalli, e che queste correnti li riscaldano, ho fatto un ultimo disperato tentativo: carta da 5000 (ovviamente praticamente scarica.. mica sono masochista) nel forno a microonde.

Cosa dovevo ottenere: In teoria l'effetto Joule sulle particelle di materiale conduttivo, presenti sulla scheda, avrebbe dovuto riscaldarle a tal punto da sciogliere lo strato di supporto e fissarle cosi' alla superfice... Cosa ho ottenuto: mia mamma che mi da dell'imbecille e niente altro. Insomma.. riuscirete a renere illegibile una scheda ma non indelebile.

MTF UPDATE - 2

Finalmente mi e' arrivato quello che aspettavo !!! Ho disponibili due testine magnetiche predisposte per leggere proprio le carte telefoniche. Collegata una di queste al mitico registratore del Commodore 64 sono venute fuori due cose:

La prima e' brutta, ovvero che la migliore qualita' di registrazione ha fatto cadere l'ipotesi che si tratti di un codice F2F. Sembra infatti (e mi e' stato confermato da un tipo esperto in queste cose) che sia una modulazione del tutto atipica.. probabilemte pensata esclusivamente per le tessere magnetiche adottate dalla telecom. (Controllando al sito della Urmet, la ditta che le produce, sembra proprio che sia un loro brevetto (vedi http://www.urmet.it). Peccato... a questo punto sintetizzare un segnale di ricarica diventa molto piu' complicato..

La seconda notizia e' pure peggio. Le testine adatte alle schede hanno un nucleo di lettura/scrittura di quasi 5mm, piu' del doppio di quelle normali.. il problema grosso riscontrato e' che la lettura avviene senza problemi, ma il circuito del registratore non ha abbastanza potenza per gestire la fase di scrittura... ovvero al massimo si riesce a cancellare la scheda... e non a ricaricarla.. Puo' essere che la carta telefonica sia pensata in modo da essere solo cancellata, ma in un mio precedente tentativo ho riscontrato la possibilita' di incidere dei segnali se il campo e' abbastanza forte.

Cosa implica tutto questo ? Che per ricopiare analogicamente una scheda e' necessario o trovare un registratore che abbia la forza sufficente o costruirsi un circuito ad hoc (cosa che va molto oltre le mie capacita').

3. Un altro Improbabile progetto di ricarica

di Turi Turi

Ho in progetto un metodo, direi light forcing, con il quale ricaricare le schede dal telefono pubblico stesso.

Il concetto e' questo: Tagliando una striscia sottile dalla scheda carica (10000), corrispondente alla banda magnetica ed incollandola in maniera provvisoria su una sceda scarica, i nuovi telefoni non si accorgono dello spessore e leggono la cifra 10000 (prova gia' effettuata su diverse cabine).

A questo punto si dovrebbe realizzare un sistema di incollaggio preciso ma 'leggero' che consenta di tirare via da sotto la testina la striscia magnetica carica. Se , come credo ,il telefono non se ne accorge comincera'

regolarmente il decremento a partire da 10000,

quindi arrivati gia' a 9800 si potrebbe interrompere la telefonata effettuata e, ritengo, che la scheda dovrebbe uscire con questo valore inciso (anche alla luce dell'MTF project).

2.3.4 Qualche nozione sulle carte magnetiche

di Master

Le carte magnetiche si dividono in due gruppi: Le carte Iso-standard e quelle band-origin.

Delle carte band-origin (carte telefoniche da 5/10m lire, viacard, airport free, Go bank, Electronic money) e'

inutile parlare ...

possiedono codici magnetici particolarissimi e leggibili solo da reader speciali non in vendita al pubblico.

Le carte telefoniche da 5/10000 lire hanno perfino una quarta traccia magnetica di protezione oltre alle tre usuali che fuoriesce dalle misure standard percui oltre al lettore speciale serve anche un particolare decodificatore URMET che la URMET di Roma appunto non vi venderebbe nemmeno se vi presentaste

travestiti da monsignore col passaporto rosso!

C'e' pero' un dato di fatto: ogni cabina telefonica possiede un lettore-scrittore della URMET!

Pero' (almeno nelle cabine un po' vecchiotte) e' ATTACCATO al telefono!!! (Fate un po' voi!!)

Questo comunica col telefono stesso tramite interfaccia RS-232 standard (c'e' perfino il connettorino supplementare... dentro!) ...averne uno da attaccare al pc potrebbe essere interessante no !?

a titolo di pura informazione nella quarta traccia (quella inscrivibile) c'e' scritto il codice 11111010110001101000 1000 uguale per tutte le carte!Sono semplicemente i numeri da 7 a 0 in fila!! (Lo puo' leggere chiunque con una lente di ingrandimento magnetica acquistabile a

l.25.000 presso qualunque negozio specializzato in automazione industriale : quelli che vendono gli orologi per il personale a schede tanto per intenderci!.)

Il codice pero' non parte su tutte le carte dallo stesso punto: e questo ha la sua influenza infatti la distanza del paccheto codice dall'inizio della banda e' a sua volta un numero che influisce sulla metodologia di interpretazione del codice stesso.

Se tagliate la banda ad una carta telefonica infatti e la riattaccate leggermente spostata (1/2 mm basta) a destra o a sinistra il telefono in cui la inserirete andra' in tilt dando valori sballati e a volte anche caratteri!

Pero' non funzionera' almeno sino a quando non rimetterete una scheda 'corretta'. Eppure su schede diverse il codice a volte e' spostato anche di un paio di centimetri!!! (Avra' la sua importanza no!?) le iso-standard sono tutte le carte che hanno il codice magnetico apposto su una fascia delle dimensioni di circa 1/4 della carta stessa distanziata 5 mm da uno dei duel lati lunghi. Su queste bande sono scritte informazioni binarie in fomato iso-standar appunto ovvero una specie di MS-DOS magnetico. Il formato ISO

e' leggibile da qualunque lettore tri-traccia (oggi tutti i

reader-writer sono tri-traccia!). La comprensione o la decodifica di questo formato e' inutile poiche' un malvivente che volesse ad esempio duplicare una carta di credito telefonico dovrebbe solo leggere il codice sulla carta con il lettore e riscriverlo cosi'-com'e' su un'altra carta bianca! (Esistono perfino writer multischeda ovvero macchinette che infilata la scheda madre da un lato ti producono 100 e piu' cloni in un colpo solo ...

queste pero'

costano in media da 5 agli 8 milioni!).

Sono iso-standard carte di credito telefoniche, carte di credito generali, bancomat, passi, e wolfer commerciali.

Un criminale che volesse copiare un bancomat in serie per poi riutilizzarlo oggi farebbe poca strada.

Facciamo un esempio: un tossico tunisino fa prendere ad un suo amico (altro tossico tunisino!) un bancomat in una banca qualsiasi (lo danno a cani e porci!). Questo se lo duplica in mille esemplari e poi col suo bel codicino regolare va in 1000 bancomat diversi e da ciascuno

preleva 500,000 lire. Questo si poteva fare solo diversi anni fa quando l'operazione sul bacomat veniva elaborata direttamente dalla carta e i movimenti diventavano effettivi presso la tua banca solo dopo 15/20

giorni. Oggi tutto e' collegato in real time percui dopo il primo prelievo le altre carte sarebebro morte!. Tanto varrebbe al tunisino far prendere al suo amico dieci o venti blocchetti di assegni per poi rivenderli o usarli cabriolet ... il reato sarebbe sicuramente

minore. (La truffa come reato e' stata anche depenalizzata... oggi e' solo reato civile... manco si finisce piu' in galera.... Un poveraccio ha un negozio di elettrodomestici... un coglione gli entra la mattina presto e gli frega con assegno a vuoto mezzo magazzino... quest'ultimo si becca solamente (se viene preso) una denuncia civile e una multa irrisoria!... bah ... che

mondo!!!)

Le carte di credito telefoniche invece funzionano ancora sul vecchio sistema.

Io ad esempio mi sono fatto una copia (e' legale questo eh!!!!) della carta di mia moglie per poter usare ambedue lo stesso numero di codice della nostra ditta. (La telecom non sente seghe.... se hai due carte devi avere due codici! oppure prendi la multiutenza che costa una

martellata sui coglioni!) L'unica cosa spratica e' che quando telefona mia moglie se io cerco di prendere la linea con la stessa carta trovo occupato. Immaginate il casino con 100 carte e piu'! La telecom non effettua il back route se non su richiesta specifica (gli costa fatica!) percui se uno telefona da Milano con un carta e poi lo stesso (o un altro per lui) telefona da Roma con la stessa carta dopo tre minuti nessuno se ne accorge. Se la Telecom volesse controllare

potrebbe effettuare come sopra detto il beneamato back route e scoprire in pochi secondi la duplicazione della carta pero'! Come dicevo prima le carte di credito telefoniche funzionano ancora con lo schema del

vecchi bancomat: voi fate le vostre belle telefonate e i soldi dal conto vengono prelevati dopo 20 giorni. C'e'

un problema dopo le prime 100.000 di spesa la Telecom vi blocca temporaneamente la scheda e vi chiede di firmare una specie di contrattino dove dichiarate che avete intenzione di usare la scheda per importi superiori.

Fatto questo avete una scheda che (per almeno 20 giorni) vi permette una mole di traffico telefonico milionaria! Non sapete nemmeno quante denuncie vengono fatte ai tunisini di cui

sopra che si duplicano le schede con questo sistema e poi fanno telefonare i loro amici al 50% delle tariffe Telecom in Africa a rotazione per 24 ore al giorno.

THE LEGEND:

La carta telefonica dentro il sale per qualche giorno o sul televisore b/n acceso da qualche ore per ricaricarla sono delle belle leggende metropolitane ...io (scemo!) ci ho pure provato .... NON FUNZIONA!!!

Non funziona con le chede scariche e non funziona con quelle che hanno ancora dentro qualche lira. E'

probabile invece che il televisore smagnetizzi quelle cariche...

questo si!!!

(E' possibile che le interferenze magnetiche del televisore modifichino l'importo della scheda a vostro favore: la probabilita' di riuscita puo' essere paragonata a quella di far centro con un bottone in una giornata ventosa dentro un bicchiere posto a dieci metri di distanza.)

Lo scotch sulla banda per non far modificare l'importo dal lettore: che cazzata!!! se il lettore non e' in grado di scrivere il codice ovviamente non puo' nenche essere in gradi di leggerlo no!!!!

3. Ed ora qualche metodo per chiamare gratis o quasi.. o no?

Qui sotto trovate qualche metodo selezionato tra quelli presenti su Spaghetti. Purtroppo la telecom sta facendo di tutto per renderli inutili.

1. Le ultime 200 lire

di Savio

Per telefonare a tempo indeterminato con una tessera servono: una cabina (non conta se nuova o vecchia, basta che funzioni a scheda), una tessera contenente almeno il prezzo dello scatto alla risposta (ad esempio 200£ per una urbana) e una tessera vuota.

Si inserisce la tessera "carica" e si compone il numero desiderato;

subito dopo si mette anche la tessera vuota tenendola ferma con un dito il più dentro possibile. Quando la prima tessera si esaurirà, verrà espulsa da sotto (NON TOGLIERLA ASSOLUTAMENTE FINO ALLA FINE DELLA TELEFONATA) e il lettore tenterà di tirare dentro la nostra seconda tessera, ma non vi riuscirà a causa del nostro dito. Ciò nonostante la comunicazione rimarrà aperta grazie alla tessera vuota (è un po' il meccanismo dell' "ultimo 1000£ nei GSM"). Quando si desidera terminare la telefonata è sufficiente riattaccare la cornetta ed estrarre le tessere.

L'unico svantaggio è che serve sempre una tessera con poco credito (vedi punto 3), ma posso assicurarvi che funziona!!!

2. Il trucco delle tre schede

di Dark Soul

Cio' che serve: una scheda da 15.000 piena (hanf hanf) e 2 sKede vuote.

Il metodo consiste nel cacciare il piu' dentro la scheda piena in modo che la legga ma che non possa piu' sovrascriversi.

Spiego: durante la telefonata vedete solo le lire che scendono, ma la tessera non si smagnetizza, bensi' questo avviene alal fine della telefonata

Per Farlo: Prendete una scheda piena da 15.000 (o 10 o 5, dipende quanto volete far durare la telefonata) e infilatela dentro, aspettate che appia sul display le lire che rimangono.

Dopo di che' infilate dentro un'altra scheda vuota, e dietro un'altra ancora.

La telefonata durera' finche' non appariranno le 0 lire sul display, e allora, quando la tessera piena dovrebbe essere smagnetizzata, viene smagnetizzata quella vuota e quella piena rimane piena.

Note: Anche in questo bisogna avere culo ma, a differenza degli altri, in questo bisogna fare anche molra pratica e bisogna essere delicati mentre si inseriscono le 2 sKede vuote.

(Questo metodo non dovrebbe più essere utile a causa del famigerato database intelligente –NdCDP).

3. Sfruttare le Carte Prepagate internazionali e le carte di credito telefoniche.

Estratto da Butchered From Inside 2

AUTORE: LeLe

CONSUMO: Qualche litro di aria

1 bicchiere di coca(ina) ;-)

1 toast

THANX: Roberta, pIGpEN, bELFy, ins4ne & BFI 98 in general.

Nel breve articolo che ho scritto ho intenzione di parlarvi della carta "CALL IT OMNIA" di Telecom Italia. Essa consente di effettuare chiamate in Italia e da/verso l'estero, addebitando la telefonata o su bolletta telefonica o su conto corrente bancario o ancora su carta di credito commerciale.
Ma se volete le solite informazioni commerciali basta che andiate a leggere pag. 17 dell'elenco telefonico. Quello che a noi piu' interessa ora e' l'aspetto tecnico-pratico.
La "CALL IT OMNIA" si presenta con le dimensioni standard di una carta di credito, con una banda magnetica sul retro. Questo particolare permette l'utilizzo della carta nelle cabine telefoniche munite di lettore apposito.
Una volta inserita la scheda, questa deve essere tolta subito e su display dell'apparecchio appare la richiesta del CU (Codice Utente) e quindi dovra' essere inserito un numero (PIN) di 4 cifre.
L'interessante della carta e' che puo' essere sfruttata senza possederla, ed anche da alcuni telefoni privati (esclusi cellulari), tramite il servizio 143.
A questo numero risponde un centralino automatico a cui dovete fornire il numero di contratto ed il PIN della ...ehm...ehm... VOSTRA carta. Il numero di contratto e' impresso sulla tessera ed ha 7 cifre.
Bisogna dire che alla Telecom non hanno capito bene cosa voglia dire sicurezza, poiche' 4 cifre di PIN non sono molto difficili da trovare con un semplice programmino.
Unico inconveniente e' che dopo il terzo tentativo non andato a buon fine, il 143 vi passa l'operatore e sfido a spiegargli che state scomodando alcune centinaia di PIN.
Un altro problemino e' dato dal fatto che l'intestatario puo' richiedere

gratuitamente la documentazione del traffico, in modo da registrare tutte le chiamate effettuate tramite la carta.

Per ovviare a questo "inconveniente" potreste inviare alla filiale Telecom di appartenenza una lettera in cui a nome dell'intestatario chiedete la sospensione della documentazione.

Il nome dell'intestatario e' anch'esso impresso sulla carta, assieme alla data di inizio di validita' della carta.

Personalmente ritengo che il sistema sia valido, specie se volete utilizzare un POP di un provider lontano da casa vostra e quindi interurbana.

In sintesi cio' che dovete procurarvi sono quanti piu' numeri di contratto possibile, poiche' per il PIN basta un po' di buona volonta'.

Grazie per il tempo che avete perso leggendo questo articolo; spero non vi abbia annoiato. La prossima volta, se ne avrete voglia, vi raccontero' qualcosa sul PNN ovvero il nuovo PIANO NAZIONALE DI NUMERAZIONE che riguardera' tutta l'Italia e rivoluzionera' il sistema attuale.

Grazie ancora e speriamo di leggerci presto nei prossimi numeri di BFI

LeLe

NOTA DI pIGpEN: Io mi permetterei di indirizzare un paio di secondi della vostra vita a questo ragazzo e alla sua buona volonta' di tirar avanti alla grande il povero pig alla fine di questo anno scolastico del cazzo, grazie davvero per il semplice fatto di averti compagno di banco :)

TELEC0M FUCKiNG UPDATE

Dopo aver letto l'articolo di LeLe (Carte di credito telefonica) vorrei fare qualche precisazione. E' vero che la carta Call It della Telecom ha la facolta' di poter essere usata senza averla tra le mani, ma conoscendone semplicemente

il codice PIN, ma questa e' l'ultima carta che utilizzerei per chiamare
gratuitamente poiche' e' quella che ti fa sgamare piu' rapidamente.
Infatti se il titolare si dovesse accorgere di qualcosa di strano sulla sua
bolletta potrebbe tranquillamente chiedere alla TELECOM la sospensione del
servizio e la notifica di TUTTI i numeri comprensivi di date e di luoghi
con conseguente sole a scacchi e sedere rosso.
Ora il punto e': la telecom cosa fa per prevenire tutto questo?
Fa indagini segrete in collaborazione con i pulotti che aspettano di beccarti
in flagrante nel mentre chiami e registrando magari le telefonate.
Quindi sconsiglio a tutti quelli che vogliano chiamare gratis di usare questo
metodo in quanto INUTILMENTE pericoloso. Lo stesso metodo descritto da LeLe
non vale mica solo per le Carte "CALL IT", ma per ogni tipo di carta PREPAGATA
emessa dalla TELECOM ITALIA. Pensate a quando partite per l'estero e vi
comprate magari all'aereoporto una bella CARTA DI CREDITO INTERNAZIONALE della
Telecom.
Il funzionamento di base e' lo stesso solo che c'e' una bella differenza, il
servizio in questo caso e' PREPAGATO e di conseguenza alla Telecom non gliene
frega un cazzo di come la usiate e nemmeno se la hanno usata a sbafo perche'
loro i soldi li hanno gia' beccati!!!!!
Mi ricordo quelle orette ai telefoni pubblici di un bel College che mi
fruttavano centinaia di crediti telefonici con conseguente chiamate gratis
a casuccia.
Il punto di vista Tecnico e' questo: Voi vi piazzate al telefono e fate finta
di parlare con mammina. Al telefono affianco compare il cazzone che deve
chiamare a casa con la sua bella tessera. 9 volte su 10 non pensa a coprirsi

il numero (PIN) e voi ve lo memorizzate (anche se e' un po' difficile) oppure ve lo appuntate in modo da non destare sospetti (magari mettendo un prefisso italiano prima e facendo finta che vi stessero dettando un numero al telefono e poi chiudete e ve ne andate. Piu' tardi andate a fare voi il numero verde della telecom che viene fornito sulla Carta (poiche' varia da paese a paese) e quando vi chiede il codice di identificazione voi ci infilate quello del CAZZONE e chiamate a spese sue!!!!

Il cazzone intanto deve fare un'altra chiamata, si avvicina al telefono, compie tutte le operazioni necessarie e si sente dire "ci dispiece comunicarle che il suo credito residuo e' terminato" con conseguente bestemmia e magari rottura del telefono (del tipo "Porca puxxana mi hanno fottuto i soldi" o "che caxxo succede avevo tanti crediti e ora non ce ne sono piu'?!?").

Se il CAZZONE e' cazzuto, al rientro in Italia si rivolgera' alla TELECOM chiedendo spiegazioni e la TELECOM non fara' niente altro che NIENTE, dicendo che la colpa e' dell'utente che non ha tenuto segreto il PIN (che in questo caso diventa di una decina di cifre e non e' personale, ma assegnato a caso dal computer della Telecom) e chiudendo li' il caso, anche perche' quelle telefonate le sono state gia' pagate.

Allora il cazzone che tutto sommato ha perso una 50ina di mila lire ci lascia stare e se ne va a casa (io dubito anche che qualcuno si sia mai rivolto alla Telecom per il rimborso scheda).

NON so se sia possibile, MA NON CREDO PROPRIO, richiedere i numeri effettuati e quindi risalire a voi, ma NON E' POSSIBILE che le autorita' vi vengano a rompere i coglioni per varie ragioni. Numero 1 voi potete sempre dichiarare di avere avuto una tessera prepagata con lo stesso PIN e di averla buttata

dopo averla esaurita (non siete mica tenuti a conservarla dopo l'uso!!)
denunciando una specie di errore di STAMPA o di assegnazione del numero con conseguente archiviazione rapida del caso e NUMERO 2 (importantissimo) il fatto e' avvenuto all'estero e la POLIZIA o FINANZA che sia non puo' indagare su fatti avvenuti all'estero.
Insomma, questo lo dico per i PARANOICI, secondo me e' piu' facile che vi sgamino in flagrante mentre vi duplicate una cassetta audio per sentirvi la musica con il walkman e vi arrestino per pirateria contro il mercato della musica (condannandovi pure!!) o che si buchi il preservativo mentre vi scopate una bellissima ragazza e vi becchiate 5 gemelli e una suocera Transex invece che vi rompano i coglioni per aver usato una prepagata altrui!!.
Il fatto interessante e' che non si possono utilizzare solo dall'estero e che la telecom italia non e' l'unica produttrice di schede del genere.
L'Italia e' uno dei pochi paesi che utilizza un sistema di schede prepagate su un supporto magnetico avendo fornito ogni cabina di un lettore (di persona ho visto un altro solo sistema del genere, si trova in Grecia e usa chip come quelli del GSM invece di supporti magnetici) a causa dell'alto costo degli apparecchi e dell'estrema facilita' di riprodurre le schede con un po' di conoscenza tecnica (e che caxxo!!!!!!) e sopratutto le macchine adeguate, di conseguenza i grandi paesi (ne cito un paio a caso: gli USA (li conoscete??) e la Gran Bretagna) hanno adottato questo sistema molto piu' semplice anche se piu' complicato da usare.
In questo modo le compagnie tipo la AT&T sono riuscite a vendere un ingente quantita' di scatti prepagati a prezzi scontati a delle compagnie che poi li dividevano in schede e li vendevano rialzandone il prezzo e "sgobbandoci su".

Le schede prepagate sono quindi vulnerabili solo per il cattivo uso fatto dai consumatori e non per la bassa sicurezza del servizio.
In questo modo negli States ho fatto incetta di carte e numeri che poi ho utilizzato anche dall'Italia chiamando gratis ovunque sul globo poiche' il numero verde da chiamare e' riportato sulla carta ed esiste in tutti i paesi del mondo (specialmente per le carte prepagate dell'AT&T) in modo da renderle utilizzabili da ogni parte del globo e a prezzi uguali per le chiamate all'estero (cosa che le carte magnetiche prepagate della telecom si sognano, al limite le puoi usare come tagliacarte all'estero :-((
Di conseguenza se volete procurarvi qualche numerino utile andate all'aereoporto internazionale piu' vicino, mettetevi ad un telefono pubblico e buon divertimento!!!!
Al piu' presto cerchero' di farvi avere una lista dei Produttori di carte di Credito Telefoniche con relativo numero verde d'accesso dall'Italia, cosi' l'unica vostra preoccupazione sara' quella di leggere il produttore (il marchio della tessera) e di copiarvi il numero di IDENT (che ho chiamto PIN per comodita').
A presto Ph d'Italia.
|PazzO| [S0ftPj98]

3. Cosa fare con il telefono

Due articoli su cosa possiamo fare di costruttivo o di distruttivo al telefono pubblico.

1. Cosa facciamo oggi al nostro amato telefono?

di Master of Puppets

Discuteremo ora di ciò che non potete fare ad un telefono pubblico: c'è un pò troppo caos, a quanto ho visto, e mi sembra giusto spiegare quali tecniche sono da relegare alla storia del phreaking.

Le tecniche che analizzerò sono le seguenti:

Boxing, Punching, Lo switch sotto al display, Storie varie con le monete, Tessere telefoniche, Danni al telefono.

Boxa tu, che io ho altro da fare

Bene, anzi, male, perchè il boxing è stato il cavallo di battaglia del phreaking per una cifra di tempo, e adesso, invece, di questo cavallo non ne è rimasta che colla. Questo è anche colpa, comunque, di tutti quei coglioni che hanno comprato una Blue per chiamare gratis, e hanno accellerato la mano di mamma Telecom nel rimodernare i propri sistemi. Quanti di questi erano Phreakers? Nessuno credo capisse come funzionasse la scatoletta magica.

Quante Box avevamo in gioco? Veramente troppe, ma le più famose sono sicuramente la Blue e la Red box, la Green, che altro non era che un mix delle prime due, e la beige box.

La Blue box non faceva altro che imitare i toni di servizio della linea (ve lo dovevo dire io?), in Italia ha avuto una vita brevissima, ma era sicura, perchè a differenza di altri stati non ti tracciavano dopo quattro minuti di stranezze rilevate sulla linea.

Non si può più usare, lo sapevate, no? I sistemi telefonici italiani sono, come dire, un pò cambiati, quindi scordatevi, cari, di downlodarvi da internet uno schema di Blue (peraltro introvabile) e di usarlo, anche perchè i telefoni, ormai, sono costruiti con filtri atti a bloccare certe frequenze...

La Red box imitava invece il rumore delle monetine che infilavi nel telefono: mi

spiego, metti 100 lire? alla centrale viene inviato il suono di frequenza XXX.
A parte che il concetto di base era lo stesso della blue (ma qui non ti tracciavano) e quindi oggi totalmente superato, tutti i progetti di red box venivano dagli USA, dove, guarda caso, le monetine, e i telefoni, sono diversi dai nostri.....
vi lascio tirare le vostre conclusioni, aggiungendo che io, ai tempi, mica c'ero arrivato, e adesso (anche prima) ho un bel soprammobile inutile.
Della Green non ne parlo neppure....
La piccola Beige Box non è altro che il lineman handset, il telefono con i coccodrilli degli omini Telecom. Nulla di speciale, un telefono normalissimo, e una box che anche un handicappato saprebbe costruirsi.
Questa funziona, ma cosa potete farci?
Prendete uno degli armadi grigi Telecom, uno di quelli dove vedete ogni tanto gli omini lavorare, e apritelo a vostra discrezione. Dentro trovate una marea di ponticelli. se vi attaccate voi , a uno di questi, avrete commesso un reato mica da ridere (come se scardinare l'armadio non lo sia), avrete occupato una linea d'utente.
Cosa fare ora? A parte non farvi sgamare dalla pula, vedete un pò voi....
Non sperate di collegarvi alla linea di un telefono pubblico perchè non funziona, ho provato sulla mia pelle, prima dal telefono pubblico a scuola, poi da un telefono pubblico dove lavoro.... beh, la linea del coso è controllata, e due telefoni connessi alla stessa linea non sono una cosa poi tanto normale.
P. S.
Se dovete telefonare, e trovate un bel lucchetto al telefono di casa, staccate la spina e sbattete nei buchi la vostra Beige... pulito, indolore, a meno che non ci sia anche la tabulazione del traffico.
Morale della favola: Se volete boxare, ma non vi piace il naso rotto e i guantoni,

fatelo in beige, che quest' anno va pure di moda...

Punching (questo sconosciuto)

Non vi è capitato quel cugino che, quando avevate quindici anni con una graffetta

telefonava a gratis? No? A me si, e quando gli ho chiesto come caxo faceva, la

risposta è stata:

La tecnica si chiama punching, e consiste nel mettere a massa il microfono del

telefono.

Prendete la graffetta fermafogli e la aprite a U.

Con una delle estremità entrate nel buchetto dove si parla della cornetta, e spingete

per rompere le protezioni e toccare la carcassa del microfono e con l'altra toccate il

cordone della cornetta.

Toh! la linea dopo un paio di sfrigolii si è liberata! Cosa faccio adesso? Sicuramente

non vado a casa.....

Non mollate la graffetta perchè se no la linea cade.....

Bene. Un metodo da paradiso, ma non funziona più, da un quattro anni circa...

Mi dispiace tanto per voi...

Tuttalpiù, se ci provate oggi, non fate altro che sminchiare il microfono, praticamente

vandalismo perfetto, invisibile e dannoso al punto giusto....metteteci anche un altra

cosetta, tipo "per qualche spicciolo in più" pubblicato su Spaghetti Phreakers", e la gente vi regalerà praticamente denaro, senza sprecarne inutilmente per le loro

telefonate...

La morale qui non esiste, gente, perchè comunque un buco oggi danneggia la

Mamma sia oggi che domani...

Almeno finchè non viene l'omino a riparare il tutto.

Lo switch introvabile

Questa storia la conoscono cani e porci: infilate una scheda tra il corpo del telefono

e il coperchio arancione proprio sopra al display, poi ravanate come quando pulite il cesso dopo una sana cagata.

Secondo il mito sotto il display dovrebbe esserci uno switch che permette di liberare la linea e parlare gratis per millenni. Si, e poi? In Sempione il fumo lo danno via gratis....

Naturalmente è una panzana galattica che non funzionerà mai. Ho provato personalmente a ravanare per ore, prima con una tessera, poi con una lamina di alluminio in caso la tessera fosse troppo corta.

Niente, non ho trovato nessuno switch, l'unica cosa che ho trovato sono le leve per riappendere il telefono, e ho chiuso la linea.

Io non ve lo dico, ma ho spezzato la lamina d' alluminio a filo del telefono e il telefono è entrato in coma: infatti da quel momento se tiravate su la cornetta era come se essa fosse comunque poggiata.

Ma. In questa storia c'è un ma. Lo switch esisteva, ed era usato per telefonare gratis.....ma dove, chiederete voi, che vado subito a telefonare?

Nei vecchi telefoni grigi, quelli di quindici anni fa...

La monetina magica (ora c'è, ora non più...e la linea cade)

Oddio, direte voi, nel telefono posso infilare le monetine, e se mi riesce con il distributore delle merendine a scuola, perchè non fottere anche lui?

Perchè? Perchè è praticamente impossibile: sui vostri soldi vengono effettuati dal telefono test assurdi, che impediscono qualsiasi contraffazione.

Primo test: peso:sembra giusto pesare la moneta per capire di che si tratta, no? quindi scordatevi di usare come metro di falsificazione solo le dimensioni, perchè vi ritrovereste con un pezzo di ferro a forma di 500 lire in mano, senza la cosa più importante, la linea.

Secondo test: dimensioni (che credevate?) la monetina viene misurata tramite un sistema di pozzetti (scivola da un pozzetto aa' latro finchè non trova quello della giusta dimensione).

Quindi, per quanto detto finora peso+dimensione= con un gran sbattimento riesco ancora a ciulare il telefono.

E invece no.

Il terzo test è il più bastardo di tutti: materiale : viene testato il materiale di cui è fatta la moneta, e qui la storia si fa dura, perchè le leghe delle monetine sono una roba impossibile da trovare.

Quindi?

Scordatevi per i succitati motivi le monetine schiacciate sotto al tram 19, e le "500 lire" fatte con lo scotch e le 50 lire, perdereste solo tempo inutilmente.

Forse la vecchia monetina col filo? Si, quella va benissimo, per far giocare il gatto...

La monetina quando la infilate nel buchetto apposito "posto sul fronte dell' apparecchio" prima di raggiungere la sezione di test viaggia in un tubo piatto fatto a forma di S. pensate che con tre metri di filo va bene? No, neppure, perchè un blocco a ghigliottina blocca la fessura per impedire l'estrazione della monetina.

Va bene, le monetine no. ma se infilo la mia mitica lamina metallica nella fessura e spingo fino a premere la levetta che dà l'accredito del denaro?

(scommetto 10'000 che 'sta idea non vi era mica venuta)

Allora ve lo eravate dimenticato il tubo piatto a forma di S !

Che facciamo allora se il bastardo non accetta le mie monetine false?

Semplice, non le acceterà più da nessuno, perchè noi prenderemo la nostra brava tessera scarica, raccolta da terra nella cabina (sempre che ne troviate, quegli avvoltoi dei collezionisti ormai battono le cabine come le troie sui viali), e la infiliamo tra il coperchio arancione e il telefono grigio.

Oooppps!! Le monetine, guarda caso, non entrano più....

La tessera ce la possiamo anche ficcare (piegata a S) nel buco da dove esce il resto , e... olè, il resto non esce più!

Pensate agli stronzi che vengono a chiamare dopo di voi, quelli PIU' stronzi, con una cifra di fretta...

Tornate dopo, naturalmente, togliete la tessera e con i loro soldi andate a bervi una birra (alla faccia loro).

Per i miscredenti, io, applicando questa tecnica del cazzo, dai telefoni sotto Duomo, a Milano, ho cacciato fuori in un ora 28'000 lire in monetanza (più qualche moneta straniera di qualche turista coglione).

La tua tessera è meglio della mia (perchè, poi?)

Ah, le tessere, cosa c'è di meglio di una tessera telefonica? Due tessere telefoniche, possibilmente riprodotte.

E invece no.

Rimarrà un sogno, almeno fino a quando non si carpirà il codice di codifica del famigerato numero di database

(prodotto per telecom da Sybase).

Intanto, uno prova di tutto, no?

No. Piantatela una volta per tutte di fare cazzate.

Scordatevi la tessera con lo scotch, se credete a queta panzana tenetevi forte, perchè sto per rivelarvi che la vera identità di Babbo Natale è Brian dei Boyzone....

Leggetevi Spaghetti Phreakers! E capirete ogni cosa!

Le due tessere sovrapposte ? Si, funzionano veramente, devo ammetterlo, se trovare uno dei lettori di tessere di sei anni fa....

Forse ,e dico forse, la tessera scarica da tenere col dito?

Un altra (purtroppo) cazzata, che non funziona più dall'ottobre di due anni fa, questo metodo l'ho provato personalmente e vi assicuro che parlavo in interurbana (da Roma, signori, mica Cologno Monzese) a Milano per due ore con 400 lire.
Poi un bel (caxo) giorno la magia è finita...e io ho ancora la mia brava tesserina bianca nel portafogli.
Ora, se volete provare, resterete al massimo a parlare in più per circa 4 minuti, poi la centrale si accorge che qualcosa non va e vi chiude il telefono in faccia....e voi non saprete mai se la tipa con cui eravate al telefono ve la darà o no.
Punto.
Cosa facciamo allora? Sicuramente se vogliamo fare del male al telefono non ficchiamo nel buco delle tessere una tessera scarica piegata in due, bensì con una siringa spruzziamo benza nel buco delle tessere, ficcate l'ago bene in fondo (ai lati, preferibilmente), e mentre spruzzate estraete lentamente.
Date fuoco, naturalmente, e, se avrete usato una siringa da pleurite rischiate che scoppia tutto, se avete usato come spero una sitinga da intramuscolo , si brucieranno le cinghiette di trasporto delle tessere, e voi sarete mooolto, mooolto contenti.
Devo darvi la morale anche qui?
Beh, ho tralasciato una cifra di trucchetti, ma tanto non funzionavano...
Ora, il gran finale.....Rendiamo il Rotorrrrr inutilizzabile
Schiacciando veloce il tasto per cambiare la lingua il telefono si impalla? Ma fateci il piacere! Vi impallate voi coi i crampi al dito, alla Remo Williams.
Allora Noi ci mettiamo l'accendino sotto . Bravi, se prima avete messo su la benzina magari succede qualcosa....
Volete danneggiare irreparabilmente un telefono?

A parte la Bombacarta da 1'500 lire nel buco delle monetine (gli dà una shekerata paurosa, e poi va in balla) prendete un pò di benza e colatela nel buco delle monete.....il danno qui è assicurato, e assolutamente invisibile.

Oppure prendete un cacciavite (ne avrete pure uno a casa, no) e ficcatelo nella tacca a lato della cornetta: forzate e rubatevi Microfono e altoparlante (un altoparlante da 200 ohm fa sempre comodo).

Richiudete il tutto e mollate li il telefono.

Se volete solo sfasciare la cornetta, perchè di materiale elettrico a casa ne avete abbastanza , tirate il cordone, e fate fare alla cornetta un paio di giri su se stessa.

Inimitabile la soddisfazione di lasciare il telefono muto!

Conclusioni (era ora)

Bene, ora che vi ho illustrato alcune delle cose che ormai vanno bene solo come fiabe per i giovani phreakers (dovreste vedere i loro occhi come brillano quando sentono certe cose) ho solo una cosa da dirvi: attenti, sempre e comunque.

A me non fotte un cazzo dei disclaimer, perchè tanto nessuno li legge mai, quindi...

2. Fregare un salvavita alla Telecom

di James Jessie

Anzitutto bisogna sapere che in ogni cabina della telecom, proprio sotto il telefono c’è una centralina elettrica contenente sia il cavo che poi si collegherà al telefono (e quindi si intravede una possibilità di collegarsi abusivamente tramite un semplice collegamento di un tel esterno, possibilmente un cordless) sia un salvavita, facilmente smontabile !!! Ora l'unico problema che si pone é come aprire la centralina, é semplice: con il semplice ausilio di uno spadino (cioè un grimaldello una chiave limata o anche solo un pezzo di ferro lavorato affinche raggiunga una forma serpentina) si agisce sulla serratura facendo un po' di gioco il risultato é assicurato all'85% !!!

P.S non é molto legale fate attenzione!!!

3. Balle spaziali

Ne girano talmente tante di bufale riguardo ai trucchi sulle cabine che abbiamo deciso di riportare qui le più gustose...

Molto casualmente, mi è capitato di riuscire a caricare, se pur di 200£ (che visto il punto 2 sono più che sufficienti), alcune schede vuote. É bastato passare sulla banda magnetica una fiamma di accendino per un paio di secondi, anche se il tempo non deve essere così fiscale, e il gioco è fatto. Purtroppo questa tecnica va a volte si e a volte no, comunque tentar non nuoce!

Prendete un televisore vecchio e accendetelo per circa due o tre ore. Trascorso tale periodo passate la tessera magnetica (con la banda magnetica rivolta verso il vetro della tv) sopra lo schermo e verificate se si e' ricaricata almeno in parte. Prima di passare la tessera magnetica sopra il televisore dategli una spruzzatina di lacca sulla banda magnatica e POI passatela sul televisore come sopra. Verificate poi anche questa.

Metodo Commodore 64

Cio' che serve: il Commodore 64 (si bravo, chiama l'amico per chiedigli se te lo presta) e una mano che vada alla velocita' di una cassetta che gira.

Un ennesimo metodo consiste nel passare la scheda sul Commodore 64 per ricaricarla.

Per farlo:

Prendete il Commodore e schiacciate il bottone REC, dopo di che' passate la scheda dalla parte della banda magnetica sul piccolo sensore dove viene solitamente letto il nastro della cassetta.

Note: La scheda deve passare alla velocita' di una nastro che gira. Fate Attenzione!!

Impallinare la macchinetta

Cio' che serve: un cervello, un dito. Uno dei modi per non pagare gli scatti e' impallinare il telefono. Occorre pero' che sia un telefono "nuovo" di quelli che vanno solo a scheda.

Per farlo:

Schiacciare MOLTO velocemente e MOLTE volte il tastino per cambare lingua mentre si parla.

Per caso stavo chiamando da una cabina pubblica, qua a Torino e mentre

stavo parlano mi son messo a stuzzicare il cello. Avevo il credito esaurito

e cosi' ho partire una chiamata premendo il stato della segreteria. Dalla

cornetta usciva un suono terribile dovuto all'effetto di Near Field, cosi'

ho cominciato a spostarlo e per caso l'ho avvicinato alla carcassa del

telefono. In pratica la macchina mi ha restituito i soldi ed e' andata fuori servizio, ma io ho continuato a parlare..

Sezione 3: L'Utenza Domestica e Internet

3.1 Introduzione

di CDP

Da Casa propria si possono fare molte cose, ma l'esperienza ci insegna che è meglio farle da casa degli altri.

Una cosa assai simpatica è attaccarsi ad una centralina telecom e scroccare le telefonate finchè non si finisce in galera, meglio ancora se si riesce a beccare la linea dell'odiato vicino, al quale si può altresì vampirare il cordless ecc. ecc. ecc.

3.2 Come funzionano le centrali Telecom

di Stefano Zano

Importante: quelle che seguono sono note pseudo-tecniche relative alla tecnologia usata da una delle compagnie che forniscono autocommutatori numerici al gestore telefonico italiano. Altre compagnie usano tecnologie differenti, ma la base e' sempre la medesima. Le variazioni sono indicate con il segno '|'

Struttura HW della c.le.

La centrale in esame e' composta da parti modulari (microprocessore,interfaccia con la rete interna, interfaccia con il mondo esterno). I microprocessori possono essere della serie 8086 80286 80386 a secondadel carico che di lavoro debbono sostenere e sono genericamente chiamatiControl Element (CE).

I CE sono raggruppati in famiglie in base alla funzione che debbono svolgere cosi' come la loro quantita' e'

determinata dalla taglia della centrale.

A seconda della modalita' di funzionamento, i CE sono suddivisi in Active-StandBy, Hot-StandBy, DuplexCE, SimplexCE, Loadsharing.

La parte periferica e' dipende dal compito che il CE deve svolgere: interfaccia con utenza normale, con utenza PABX, con canali PCM, con dispositivi di massa, ecc

L'Hw delle periferiche e' costituito prevalentemente da componenti custom cioe' costruiti appositamente per svolgere funzioni telefoniche.

Una centrale e', schematicamente, composta da:

PLCE Active-Stby Gestisce le memorie di massa di c.le, interfaccia l'operatore, carica gli altri CE della centrale

| DFCE " " Gestisce la parte di manutenzione e allarmistica della centrale

| CTCE Hot-Standby Gestisce tutte le temporizzazioni, genera i toni e le correnti, gestisce (per ora) gli annunci di cortesia

CHRG " " Gestisce la tassazione e tutto cio' che e' ad essa associata

ADMIN " " Gestisce la parte amministrativa: documentazione traffico, utenti sotto controllo ecc.

PATED LoadSharing Analisi delle numerazioni ricevute, prima scelta per l'instradamento.

SVCE " " Gestione delle segnalazioni DTMF tra utente e centrale

TRA Hot-StandBy Supervisione dei canali di connessione centrale -centrale

CEPBX Active-Stby Gestisce i PBX della centrale

LTCE Active-Active Gestiscono gli attacchi d'utente.

EISM " " Gestiscono sia attachi d'utente normale che ISDN

MPX " " Modulo con 30 utenti remoti

ERSU/IRSU " Modulo con 488 utenti remoti

DTM SimplexCE Gestiscono fisicamente i canali tra c.le e c.le

CCSM SimplexCE Gestiscono i link di segnalazione in canale comune

N7O DuplexCE Supervisore di tutti i CCSM

TTM SimplexCE Prova automaticamente tutti i canali della c.le

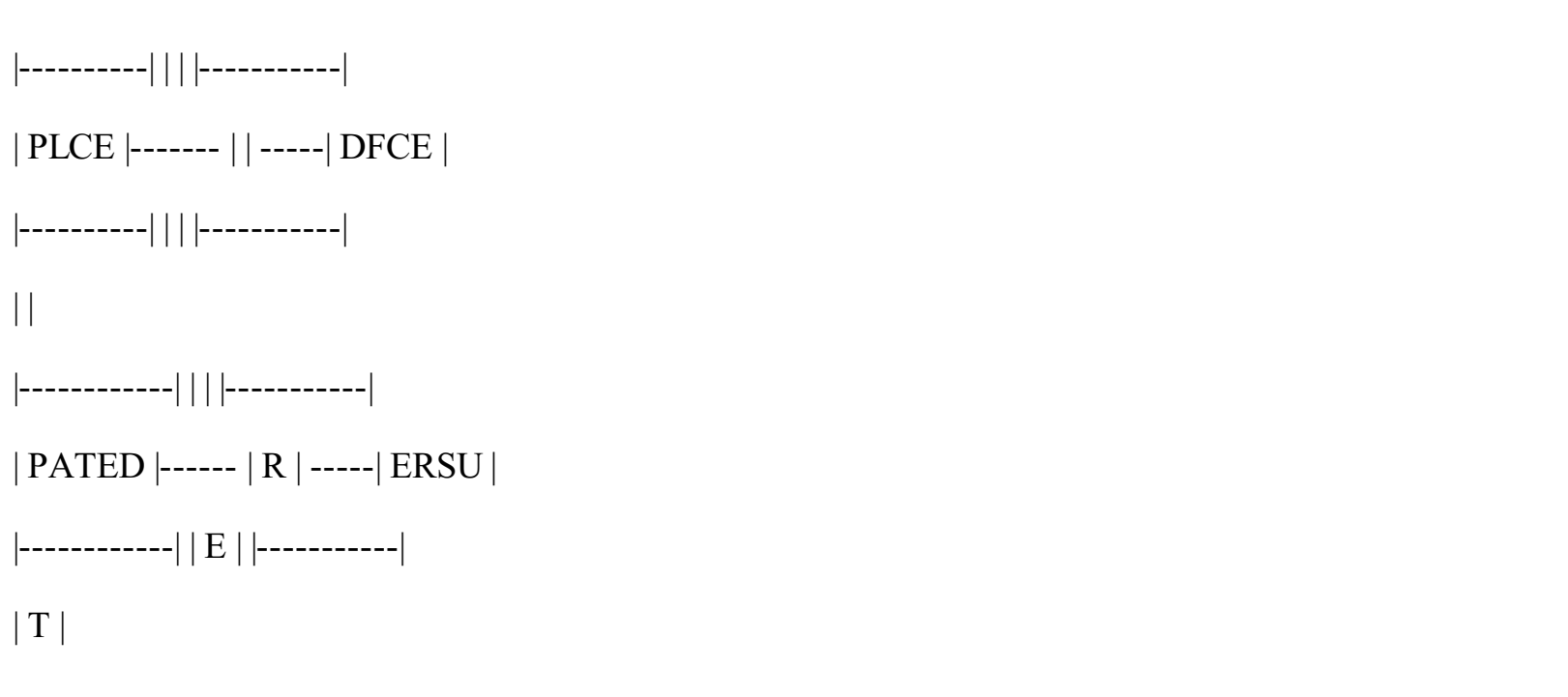
PTCE SimplexCE Dialogo Man-Machine in modo avanzato.

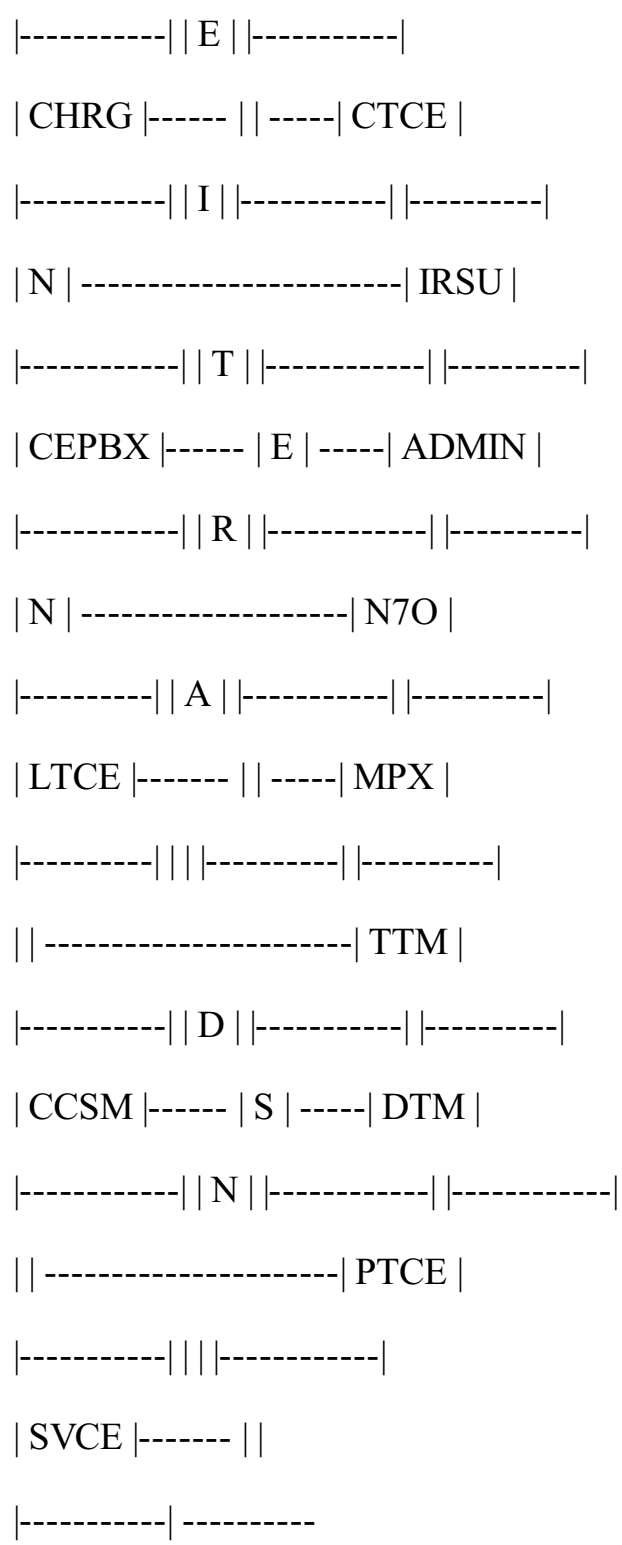
Ogni modulo LTCE gestisce 128 utenti per cui ne saranno equipaggiati in quantita' tale soddisfare le esigenze del gestore del servizio I moduli DTM gestiscono 30 canali PCM ciascuno e anche di questi ne saranno equipaggiati una quantita' tale da soddisfare le necessita' del traffico previsto e delle direzioni da gestire.

Gli altri moduli sono in coppia (Active-StandBy) o singoli (SimplexCE) La funzione di Active-StandBy viene implementata per quei processori in cui deve essere garantita al massimo l'affidabilita', cioe', se un CE va fuori servizio, il suo partner deve essere in grado di gestire le funzioni di entrambi i CE

Nelle centrali di grossa taglia o con particolari funzioni sono presenti altri tipi di processori che, sostanzialmente, svolgono alcune funzioni solitamente incorporate nei processori utilizzati per le piccole taglie. Sono poi equipaggiati processori che servono a funzioni ausiliarie e/o per collegamenti con i centri di manutenzione/supervisione.

Diagramma a blocchi di una centrale





In realta', bisognerebbe interpretare la centrale come un cerchio (la rete) attorno a cui sono collegati i vari processori, non essendoci alcuna gerarchia tra i vari CE e gruppi di CE

I processori non hanno un collegamento rigido tra di loro, tutte le informazioni vengono scambiate tramite messaggi. La struttura di questi messaggi e' custom e non segue alcuna specifica internazionale.

Lo scambio di messaggi avviene tramite rete sfruttando link a 4 Megabit e porte (switch) gestite da processori custom. Ogni processore puo' gestire 16 porte (00 - 0f); ogni porta costituisce un indirizzo fisico e la capacita' massima di indirizzamento e' di 65536 (FFFFH) porte.

Attualmente (e non succedera' mai) nessuna centrale, per quanto grande, utilizza tutti quegli indirizzi.

La rete interna della centrale (DSN: Digital Switching Network) e' costuita da vari stadi, piani e gruppi. La quantita' di questi e' determinata dalla taglia della centrale.

Il software di centrale

La parte elaborativa e' affidata al software. Ogni CE ha il proprio SW e il proprio FW specifico, in funzione del lavoro che deve svolgere. Esiste, inoltre, del SW che non appartiene a nessun modulo ma che e'

utilizzato da diversi CE e che viene richiamato solo quando necessario.

Infine c'e' il SW per il dialogo man-machine che si puo' considerare suddiviso in due parti: una parte per la gestione da operatore della centrale, l'altra per una manutenzione spinta effettuata da tecnici specializzati.

Linguaggio SW utilizzato

Il linguaggio SW utilizzato in questo tipo di centrale e' di tipo proprietario ed e' chiamato CHILL

(Communication High Level Language). Il CHILL e' solo codice, tutta la struttura dati e' costituita da tanti files di database a cui CHILL accede mediante opportune chiamate.

Esiste anche un altro tipo di SW che e' quello di controllo e supervisione del database. Ogni variazione al database puo' essere eseguita solo se sono rispettati tutti i criteri di validita' della

operazione. Il DBMS (Data Base Management System) verifica che tutte le chiamate ai files di database siano corrette, che tutti i files vengano aperti e chiusi in modo regolare, che non ci siano sconfinamenti ecc.

ecc. Se una chiamata non e' corretta, la variazione non viene accettata, viene generato un report di errore e viene ripristinata la situazione precedente.

Come gia' detto, ogni CE ha il proprio SW. Questo SW e' suddiviso in due parti: SSM e FMM.

Le SSM (Simple State Machine) hanno il compito di fare da interfaccia tra la parte HW e le FMM (Finite Module Machine) le quali hanno il compito delle elaborazioni ad alto livello e di dialogo tra i vari CE.

Le FMM possono essere di tipo reale o di tipo overlay. Il tipo reale ha una collocazione ben precisa nella memoria del processore, il tipo overlay viene caricato solo al momento del bisogno in una zona riservata della memoria e li risiede finche' non viene caricata un'altra overlay.

A loro volta le SSM, le FMM e gli overlay sono suddivise in tre parti:

-Una parte fissa detta GLS che non viene mai modificata se non perinserire dei JMP alla parte

-APATCH contenente una serie di patches atte a risolvere un malfunzionamento o ad adattare il GLS

(comune tra tutte le compagnie dellamultinazionale) alla realta' italiana. Nelle APATCH sono contenute solo le correzioni accettate dal gestore del servizio telefonico, altre patches sono inserite nella parte

-UPATCH che contiene patches 'in prova' e che se validate passeranno nella parte APATCH, altrimenti verranno rimosse senza compromettere il funzionamento della parte esistente.

Ogni CE ha mediamente una ventina di FMM, una decina di SSM, una decina di overlay e 100/150 files di database. I files di database sono racchiusi in un unico file chiamato DLS (Data Load Segment). I files di codice sono racchiusi in tre files:

-GLSC contiene i GLS common

-GLSP contiene le APATCH

-GLSU contiene le UPATCH

Ogni volta che un processore viene caricato, nella sua memoria vengono inseriti questi 4 files piu' alcune tabelle di distribuzione per la gestione dei CE di tipo centralizzato.

I files di codice sono comuni per ogni processore appartenente alla stessa famiglia (i LTCE avranno tutti lo stesso codice: debbono fare tutti la stessa cosa); i files DLS variano da processore a processore (il primo LTCE e' equipaggiato in una posizione diversa dal secondo LTCE, gestisce attacchi d'utente diversi, ecc per cui i dati devono essere necessariamente diversi)

In una centrale con 100 LTCE saranno quindi presenti 100 DLS. In realta' i DLS presenti sono solo 50 in quanto ogni LTCE e' in grado di gestire anche gli utenti "di suo fratello" (discorso che verra'

affrontato piu' avanti) per cui in caso di down del CE, "suo fratello" si fa carico della gestione dei propri 128

utenti, piu i 128 del CE Down.

Files di overlay

Come detto piu' sopra, nei vari CE vengono caricati anche dei files di tipo overlay. Queste parti di codice non servono al funzionamento telefonico del CE, ma vengono caricati quando necessario.

Solitamente sono overlay tutti i files che contengono il codice per la gestione dei comandi da operatore oppure quei files preposti alle funzioni amministrative: gestione dei contatori, dialogo Man-Machine, dialogo con il centro di supervisione, ecc

Utenti

Gli utenti sono coloro che tramite un contratto con il gestore del servizio possono collegare il loro terminale (telefono, fax, modem o altro) alla centrale telefonica e avere la possibilita' di dialogare

con un altro utente o macchina.

Vi sono varie classificazioni per gli utenti:

- Simplex

- Duplex

- PABX (a sua volta suddiviso in vari gruppi)

- ISDN (anche questi si suddividono in vari gruppi)

Ogni utente e' caratterizzato in modo univoco, nei confronti della rete telefonica mondiale con un identificativo composto da una serie di cifre. Tali cifre indicano il codice nazionale, il codice del distretto, il codice personale assegnato all'utente.

L'utente ha, poi, un suo profilo, cioe' una serie di parametri che ne stabiliscono le facility e/o la segnalazione che puo' utilizzare per poter accedere alla rete pubblica.

Il profilo dell'utente e' modificabile su richiesta dell'utente stesso, oppure dalla amministrazione dal gestore del servizio.

Per le nostre elucubrazioni parleremo sempre di utente con le seguenti caratteristiche:

- simplex con segnalazione DTMF

- senza alcun servizio STS

- abilitato a trasmettere e a ricevere

- le chiamte effettuate/ricevute sono nell'ambito della stessa rete

urbana.

Eventuali variazioni del profilo verranno discusse mano a mano che il discorso evolve.

Segnalazione DTMF e decadica

L'utente telefonico utilizza il telefono per comunicare verbalmente con il proprio prossimo.

Per poter stabilire la connessione verbale compone l'identificativo dell' utente con cui desidera colloquiare.

La composizione dell'identificativo avviene, negli apparecchi moderni, tramite la pressione di tasti.

Alla pressione di un tasto si hanno due possibilita'

- Il telefono e' caratterizzato a selezionare in decadico:

Le cifre sono trasmesse in linea tramite aperture e chiusure del doppino (i due fili, di solito bianco e rosso che il gestore del servizio prolunga dalla centrale fino a casa dell'utente) La segnalzione decadica e'

composta da tre parametri

- tempo di impulso

- tempo durante cui il doppino e' chiuso

- tempo di pausa

- tempo durante cui il doppino e' aperto

- tempo di intercifra

- tempo che intercorre tra una cifra e l'altra.

I valori di targa sono: 50 millisec per impulso e pausa; 800 millisec per l'intercifra.

Nella realta' si utilizza un rapporto 40/60 per impulso/pausa e 700 millisec. per intercifra.

- Il telefono e' caratterizzato a selezionare in multifrequenza (DTMF)

In questo caso vengono mandati in linea una serie di frequenze, opportunamente modulate tra loro, rappresentanti la cifra selezionata o i tasti ausiliari '#', '*', 'R' e 'RP'.

Le frequenze sono state scelte in modo da evitare il piu' possibile che ci siano mescolamenti con la voce umana.

Fasi della chiamata

Una chiamata puo' essere scomposta in 5 fasi principali che a loro volta sono suddivise in sottofasi che possono essere suddivise ... fino a raggiungere un livello detto primitivo.

Le fasi principali sono:

- Sgancio

- Selezione

- Fine selezione

- Risposta

- Tassazione

- Riaggancio

Queste fasi sono quelle note all'utente che desidera entrare in comunicazione con un altro utente. Esistono un'altra serie di operazioni che vengono eseguite dalla centrale in funzione della chiamata effettuata oppure vengono effettuate in modo autonomo nell'arco della giornata o in un periodo prefissato.

Sgancio e preselezione

Tutti i corsi di telefonia iniziano con la seguente frase: L'utente sgancia il microtelefono ... e da questo momento inizia il caos :-)))

Cosa succede quando l'utente alza il microtelefono??? Si sente il tono di centrale (o meglio, di invito a selezionare) rispondono tutti. Verissimo, ma nel frattempo sono state eseguite moltissime operazioni sia HW

che SW.

L'attacco d'utente su cui e' attestato il nostro abbonato ha delle sonde sempre attive che in un qualunque momento sono in grado di rilevare le variazioni di corrente prodotte dallo sgancio del

microtelefono.

| Quando viene rilevata una di queste variazioni, tipicamente di circa 20 milliampere, viene attivata una SSM

che tramite opportuni algoritmi e' in grado di stabilire l'identita' logica di chi ha sollevato il micro.

Attenzione: per la centrale il numero telefonico dell'abbonato non esiste, l'utente e' sempre identificato con una associazione EN+TN dove EN rappresenta il codice logico del LTCE su cui e' attestato l'utente e il TN e'

il Terminal Number all'interno di questo EN. L'associazione tra EN+TN e numero telefonico (DN) viene fatta solo al momento di registrare sulle memorie di massa i contatori degli scatti oppure quando e' necessario inviare l'identificativo del chiamante alla parte terminale.

Una volta rilevata l'identita' viene interrogato il database (DLS) del LTCE per individuare il profilo dell'utente.

La prima cosa che viene verificata e' se l'utente e' autorizzato ad effettuare chiamate

uscenti.

Se la ricerca ha esito negativo il LTCE, mediante rete interna invia al modulo CTCE un messaggio con l'ordine di prolungare verso l'utente un tono di congestione o un messaggio fonico di cortesia (caso di utente moroso).

In caso di esito positivo, viene analizzato il tipo di segnalazione che l'utente potra' utilizzare, gli STS presenti, l'appartenenza o meno ad utenza multilinea ed altre informazioni utili per il proseguimento

della chiamata.

Tutte queste informazioni vengono inviate al PATED che, analizzando il proprio DLS, ricerca le caratteristiche generali dell'utente al fine di

 verificare le compatibilita' tra le informazioni ricevute e i propri dati interni,

 si predispone a ricevere le cifre,

 informa il modulo SVCE di predisporre dei ricevitori multifrequenza per la traslazione delle cifre e infine

 informa il CTCE di prolungare il tono di centrale verso l'utente.

Supponendo che le tutte le risorse siano disponibili:

- SVCE analizza il proprio DLS e cerca un ricevitore multifrequenza disponibile, trovatolo ne invia l'identita' al PATED che predisporra' un cammino EN+TN - SVCE

- CTCE tramite opportuni comandi alla rete interna predispone il cammino fisico tra il generatore dei toni e l'interfaccia CE - DSN. Il CE, a sua volta, predispone il percorso tra l'attacco d'utente e DSN.

Al termine di queste operazioni l'utente riceve il tono di invito a selezionare. (Nel caso in cui l'utente abbia il Trasferimento di Chiamata attivo gli viene inviato un tono continuo).

Selezione

LTCE fa partire un timer di attesa cifre allo scadere del quale, se nessuna cifra e' stata selezionata, invia un messaggio al PATED di rilasciare tutte le risorse predisposte; contemporaneamente informa il proprio livello basso (SSM) di commutare dal canale in cui e' presente il tono di centrale al canale in cui e' presente il tono di congestione (in questo caso si chiama di incapsulamento: l'utente viene isolato dagli organi di centrale fino al riaggancio del microtelefono).

L'utente compone la prima cifra. LTCE, essendo una selezione DTMF, si rende trasparente e lascia che le frequenze arrivino al ricevitore del SVCE; nel frattempo resetta il timer di attesa prima cifra e fa partire un timer di intercifra scaduto il quale si comporta come se nessuna cifra fosse stata selezionata. SVCE verifica che le frequenze siano corrette. Se non lo sono le scarta e si mette in attesa di frequenze corrette. Alla ricezione delle frequenze corrette le trasforma in numeri e le passa al PATED. PATED inizia la scansione dell'albero di selezione fino a che non trova la cifra corrispondente a quella ricevuta, verifica se l'informazione ricevuta e' sufficiente o meno per instradare la chiamata. L'informazione non e' sufficiente, quindi manda a SVCE la richiesta di

ritornargli una ulteriore cifra. Se SVCE ha nel frattempo ricevuto una ulteriore cifre la passa al PATED, altrimenti si mette in attesa pure lui.

L'utente nel frattempo ha selezionato un altra cifra, SVCE la inoltra al PATED il quale, dal punto il cui il puntatore si era fermato in precedenza, inizia una scansione all'interno di quella maglia.

Ulteriore verifica se le cifre sono sufficienti: supponiamo lo siano. PATED informa SVCE di tenere memorizzate tutte le ulteriori cifre che ricevera' da LTCE e all'interno del database va a raccogliere le informazioni necessarie all'instradamento della chiamata.

Viene letto il codice della destinazione, il numero minimo e massimo delle cifre da inviare alla parte chiamata, il tipo di tassazione e un codice per reperire i dati di interlavoro.

Vediamo un attimo, in breve, il significato dei codici letti.

Codice della destinazione: informazione ad alto livello per poi reperire i canali fisici su cui far transitare la chiamata.

Numero cifre da inviare: rappresenta il minimo/massimo numero di cifre che e' necessario mandare alla

parte chiamata affinche' sia in grado di poter raggiungere l'utente di destinazione

Dati di tassazione: ad ogni numerazione e' asociata una tassazione in funzione del punto di arrivo della chiamata (locale, urbana, urbana TUT, distrettuale ecc ecc)

Dati di interlavoro: contengono tutti dati per far si che la chiamata possa andare a buon fine in funzione della segnalazione presente sulla tratta tra le due centrali, sulle cifre da aggiungere/modificare/sopprimere, quando e come dare il comando di fine selezione, in che modo gestire la risposta, sopprimere o meno i PAD

per l'echo ecc ecc

Torniamo al nostro PATED che e' ancora alla ricerca di tutti i dati necessari al prolungamento della chiamata. Come prima cosa informa il CHRG di predisporre tutto quanto gli compete affinche' la chiamata abbia la corretta tassazione.

CHRG in base al codice ricevuto va ad analizzare il proprio database e ricerca i dati corrispondenti al codice ricevuto. In questi dati e' scritto quando e come tassare, lo scaglione da applicare ecc ecc.

PATED esegue una ricerca interna per rintracciare, in base al codice di destinazione, le caratteristiche del fascio di canali che saranno impegnati dalla chiamata: tipo di segnalazione, tipo di ricerca dei canali, CE

TRA che supervisionera' i canali ecc ecc Una volta lette queste informazioni, PATED informa TRA richiedendogli notizie sullo stato dei canali del fascio necessario alla nostra chiamata. TRA, in base al codice del fascio ricerca quanti canali sono liberi e su quale

DTM e' possibile rintracciarli.

Se il fascio di canali prevede che questi debbano lavorare in canale comune, viene avvisato il CE N7O

affinche' si predisponga a riservare uno slot in un link di segnalazione di quel fascio: viene raccolto il codice della centrale originante e quello della ricevente e li invia al CE CCSM.

Nel frattempo PATED ricerca i dati relativi agli interlavori cosicche' quando sara' possibile predisporre il canale per trasmettere le ulteriori cifre sia possibile predisporre anche le altre informazioni per il corretto completamento della chiamata.

Il TRA controllando nel proprio database, avra' gia' rinracciato un canale libero appartenente al fascio interessato alla chiamata.

Informa il CE DTM, il CCSM e il PATED.

CCSM predispone l' associazione canale fonico con slot-link di segnalazione, DMT si predispone al perfezionamento del collegamento fonico in funzione dei dati di interlavoro che PATED gli avra' inviato.

A questo punto e' tutto pronto affinche' la connessione con l'altra centrale sia possibile.

Il link CCSM invia un messaggio alla centrale a lui adiacente e gli comunica che e' in arrivo una chiamata

(fare attenzione ora) per la centrale il cui codice e' quello indicato nel messaggio.

Come e' possibile notare, ho scritto "... per la centrale..." anziche' utente in quanto e' necessario prima stabilire la connessione fisica tra i vari autocommutatori.

Quando la centrale di destinazione riconosce che il messaggio partito dal nostro CCSM contiene il proprio codice di identificazione, informa la centrale di partenza che e' pronta a ricevere le cifre.

Il link tra le varie centrali e' gia stabilito. A questo punto il PATED originante avvisa SVCE di inviare le eventuali cifre che sono state selezionate dall'utente.

SVCE invia le cifre al CE N7O che le inserisce in un messaggio e tramite l'accoppiata CCSM-DTM le cifre sono a disposizione per essere inviate a destinazione.

Nota: In realta' le cifre vengono (quando possibile) inviate con il messaggio di impegno dei vari link, risparmiando cosi' ulteriore tempo di occupazione di organi comuni.

Noi supponiamo invece che il nostro utente invii le cifre con molta lentezza e per di piu' ne mandi una quantita' superiore a quella richiesta.

Fine Selezione

Dopo il messaggio "OK il link e' stabilito" vengono inviati tanti messaggi quante sono le cifre che l'utente ha digitato. La centrale di destinazione impegna un proprio LSIF (Modulo SW del

PATED) ed inizia ad analizzare le cifre ricevute. Anche in questo caso, come nel lato uscente, viene scandito l'albero di numerazione della centrale. Le cifre ricevute non sono ancora sufficienti: viene mandata a ritroso la richiesta di una ulteriore cifra. La cifra viene inviata. Questo si ripete fino a che LSIF non ha raggiunto il numero massimo di cifre previsto.

A questo punto viene inviato a ritroso un messaggio di Fine selezione che sostanzialmente sta ad indicare

"Non mandarmi altre cifre perche' non mi servono e non saprei che farmene".

La centrale originante smette l'invio e le eventuali ulteriori cifre ancora memorizzate vengono rimosse da SVCE, quindi si mette in attesa degli eventi.

La centrale terminante con le cifre ricevute analizza il proprio database ed individua il modulo e il TN

(EN+TN) su cui e' attestato l'utente chiamato, vengono lette le caratteristiche dell'utente per verificare che sia in grado di ricevere la chiamata e si controlla che non ci siano particolari Servizi Telefonici Supplementari (Trasferimento di chiamata, Call Diversion ecc).

Se l'analisi e' positiva, viene inviato un messaggio a LTCE di preparare un cammino tra CE DTM e EN+TN; viene inviato un messaggio a CTCE affinche' predisponga l'invio del tono di libero al chiamante e della corrente di chiamata (per far squillare la suoneria) al chiamato.

(Nel nostro esempio si suppone che l'utente chiamato sia libero. Nel caso di occupato viene letto il database dell'utente per verificare la presenza del servizio di chiamata in attesa o di CCBS e si procede

di conseguenza)

Risposta

L'utente chiamato risponde. Le sonde HW si accorgono della variazione di corrente e informano LTCE della avvenuta risposta. LTCE manda un messaggio a ritroso che tramite i link di segnalazione arriva fino alla centrale chiamante.

PATED, ricevuto da CCSM il messaggio di risposta avvisa il CHRG di incrementare di una unita' il contatore dell'utente e, in base al codice ricevuto in precedenza, di applicare le ulteriori tassazioni.

Gli utenti sono in grado di comunicare, gli organi centralizzati (PATED SVCE, CTCE, N7O) vengono rilasciati e sono pronti per nuove chiamate.

Tassazione

Come detto, come viene ricevuto il criterio di risposta PATED invia a CHRG il messaggio di incrementare di una unita' il contatore dell'utente e di predisporsi ad eventuali tassazioni multiple.

L'attivazione o meno di eventuali attivazioni e' data a CHRG da PATED appena questi e' in grado di instradare la chiamata.

Oltre ai dati della tassazione viene analizzato anche il momento in cui si svolge la chiamata: anno mese giorno ora e minuti. Unendo queste informazioni con quelle ricavate dall'analisi del codice ricevuto da PATED, CHRG e' in grado di effettuare una tassazione corretta e precisa.

I tipi di tassazione sono cinque da cui discendono tutti gli alri a seconda di tempo, distanza ecc.

1 - Senza tassa

2 - Tassa fissa

3 - Un solo scatto alla risposta in chiamata urbana

4 - Tariffa Urbana a Tempo

5 - Ciclica

Le chiamate in cui non e' prevista alcuna tassazione sono quelle relative ai servizi di emergenza (112 113

115 118 ...) e ai cosidetti numeri verdi (167x). Mentre nel primo caso la chiamata non ha realmente alcuna tassazione, nel secondo caso, la tassa viene attribuita all'utente chiamato detto anche FI (Fornitore dell'Informazione).

Nel caso di chiamate a servizi di decade 1 (servizi speciali) la tassa prevista (da 1 a 5 scatti) viene addebitata al momento della risposta. Fa eccezione la telelettura del contatore (1717) dove la tassa viene applicata al riaggancio della chiamata.

La condizione di un solo scatto alla risposta in caso di chiamata urbana, la si puo' definire "una razza in

via di estinzione".

In questo caso viene attribuito un solo scatto alla risposta e il resto della conversazione urbana e' gratutita. Il gestore del servizio applica una sovratassa forfettaria cosicche' la bolletta media equivale

a quella di un utente che riceva la tassazione TUT.

La TUT (Tariffa Urbana a Tempo) e' la tassazione che viene applicata, dove prevista, alle chiamate urbane.

A differenza della ciclica e' sincrona con la risposta, cioe' il secondo impulso di tassa viene addebitato esattamente allo scadere del timer stabilito per quella fascia oraria. La tassazione ciclica viene applicata per tutte le chiamate con tasazione multipla (esclusa la TUT). In questo tipo di

addebito il secondo scatto non e' sincrono con la risposta, ma puo' essere attribuito nel periodo di tempo compreso immediatamente dopo lo scatto alla risposta e lo scadere del timer previsto per quella tariffa.

Lo sfalsamento del secondo scatto e' dovuto al fatto che questo tipo di tassazione e' generato da un tool SW

che in continuazione indipendentemente dalle chiamate che sono attive.

Gli scatti successivi al secondo avranno sempre la cadenza prevista dalla tariffa in corso.

CHRG ha tutte queste informazioni nel suo database ognuna delle quali e' codificata e quindi quando riceve il codice da PATED e' in grado di applicare immediatamente la tassa corretta.

Riaggancio

Al termine della conversazione gli utenti si scambiano i saluti e decidono di riagganciare il microtelefono.

Il chiamante riaggancia per primo. L'HW di EN+TN rileva l'apertura del doppino inviando un messaggio interno a LTCE. LTCE informa immediatamente CHRG di fermare l'addebito degli scatti al chiamante, invia un messaggio a DTM informandolo dell'evento di svincolo e rilascia tutte le varie connessioni interne.

DTM, intanto, invia sul link di segnalazione un messaggio di svincolo in avanti. La centrale ricevente informa il proprio LTCE dell'evento. LTCE apre un canale tra CTCE e utente cosicche' questi possa inserire sulla linea del chiamato un tono di congestione.

LTCE informa DTM dell'operazione e DTM invia a ritroso un messaggio di controllo svincolo quindi libera i canali verso la centrale a monte e il treno interno fino a LTCE che supervisiona l'utente per un altro minuto aspettando che questi riagganci, poi chiude il canale con CTCE e libera la linea mettendola nello stato di

"Available Busy", stato da cui uscira' appena in chiamante riappende il ricevitore.

La centrale a monte, nel frattempo ha gia' liberato tutti i vari canali cosicche' sia l'utente chimante che

sono di nuovo disponibili per una nuova chiamata.

Il chiamato riaggancia per primo. L'HW di EN+TN rileva l'apertura del doppino inviando un messaggio interno a LTCE. LTCE invia un messaggio a DTM informandolo dell'evento di riaggancio del chiamato.

DTM invia un messaggio N7 al DTM a monte informandolo che c'e' stato uno svincolo a ritroso quindi di non chiudere i canali.

DTM della centrale a monte informa il proprio LTCE dell'evento.

LTCE fa partire un timer detto di attesa seconda risposta. Se il chiamato risolleva il ricevitore, tutto riprende come prima annullando tutti i messaggi di svincolo.

Se invece scade il timer, LTCE abbatte la linea del chiamante, informa CHRG di terminare la tassazione in corso e invia un messaggio a DTM di inviare a valle un messaggio N7 di svincolo forzato. Con questo tipo di messaggio tutti i cammini vengono resi disponibili senza attendere i

normali riscontri.

Contatori in memoria CE e memoria di massa

Ogni LTCE conserva in memoria il valore dei contatori relativi agli EN+TN che deve gestire.

Questi contatori vengono letti ad intervalli regolari dal CE CHRG con un sistema di polling, quindi trasferiti alle unita' dischi della centrale. Il trasferimento LTCE-CHRG-DISCHI si ha, invece,

autonomamente ogni volta che il valore del contatore in memoria raggiunge un valore predefinito (tipicamente $FF).

In questo caso, LTCE richiede a CHRG una lettura forzata del blocco di contatori, CHRG effettua la lettura dei contatori e li trasferisce alla memoria di massa.

Ogni LTCE ha, in memoria e aggiornati, i contatori del LTCE suo partner nell'azione di crossover (un CE

gestisce tutti i 256 utenti della coppia in seguito al down del partner). Questo evita la perdita dei contatori nel caso di down di uno dei due LTCE. Nel caso di down di entrambi i LTCE della coppia, vengono tenuti validi i valori del poll precedente e salvati sui dischi. Quindi la perdita massima e' data dal delta tra il valore sui dischi e il valore in memoria al momento del crash.

Ad ulteriore garanzia ogni 6 ore i valori dei contatori sui dischi vengono travasati anche su unita' magnetiche a nastro. Questo permette anche di avere una cronistoria, in caso di necessita', della

progressione dei contatori.

Tutte le notti, poi, il centro di sorveglianza regionale contatta tutte le centrali della zona e acquisisce i files dei contatori per poi passarli alle varie elaborazioni, prima fra tutte un incremento anomalo dei valori tra due periodi di tempo.

Spiegazione di alcune sigle utlizzate

Il suffisso CE che appare in molte sigle sta a significare "Control Element" (Elemento di controllo o processore). In alcuni casi (Admin, Chrg...) il suffisso non compare, va pero' inteso come se fosse presente PLCE Periferal & Load

DFCE Defence

CTCE Clock & Tone

CHRG Charging

ADMIN Administrator

PATED Prefix Analisys and Device inetworking data analisys

SVCE Service

TRA Trunk Resource Allocator

LTCE Line Terminal CE

EISM ELC I-family Subscriber Module

MPX MuX Peripheral

ERSU/IRSU ELC/I-family Remote Subscriber Unit

DTM Digital Trunk Module

CCSM Common Channel Signalling Module

N7O N7 Overview

TTM Trunk Test Module

PTCE Peripheral

GLS Generic Load Source

APATCH Accepted Patch

UPATCH Unaccepted Patch

EN Equipped Number

TN Terminal Number

DN Directory Number

LSIF Local Subscriber Interface

3.2 Internet Gratuita

Se un tempo col proprio modem ci si collegava alle BBS, oggi ci si collega ad internet, ma i costi sono molto alti, vuoi per la TUT, vuoi per gli abbonamenti salatissimi agli ISP. Come fare per ovviare a queste cose?

Sgamare la password di un altro o usare i famigerati green….

3.3.1 Cosa sono i Green

di CDP

Questo me l'hanno chiesto in molti… e mi viene da rispondere che chi non lo sa non dovrebbe neanche usarli. Infatti secondo molti l'esistenza di questi green dovrebbe essere tenuta il più segreta possibile e probabilmente non hanno tutti i torti…

Comunque sia, un green è un numero verde che da' accesso ad internet, avendo un appropriato account, ma in alcuni casi non c'era bisogno neanche di quel o, vedi il famigerato green del a TIN.

Il perché dell'esistenza di questi numeri è vario e a volte misterioso.

In alcuni casi si tratta di provider che effettuino questo servizio su pagamento, in altr il numero dovrebbe essere a conoscenza solo degli operatori di questi ISP, in altri ancora il numero è stato messo su per altri scopi con dei 'buchi' che hanno consentito lo scrocco dell'accesso al a rete.

A tale proposito sentite quanto riporta Fab:

"L'167012837 e' un numero verde di servizio telecom dislocato a Cagliari rispondente al dominio 194.20.32.X di classe C, ovviamente. Il router che risponde non e' un cisco ma un ascend.

Il numero, fino a 2 mesi fa, aveva permesso a molta gente di navigare a gratis in rete grazie a qualche pirla della telecom che aveva messo un proxy http/ftp su delle HP presenti nel loro centro

macchine. Se una volta entrati sull'ascend (bastava far aprire la finestra terminale dopo la connessione) si controllavano le tabelle di routing si accorgeva che alcune macchine esterne erano visibili; in particolare 195.31.190.135 che aveva la solita porta 8080 aperta.

Tutto questo e' durato esattamente dal 22 Dicembre fino a meta' Marzo.

Comunque sia su tale numero, molto prima della scoperta del proxy, si erano stabilite piu' persone che utilizzavano tale numero per chattare, scambiarsi file,...etc.... Purtroppo tutto cio' non e'

piu' possibile in quanto oltre alla divisione in 4 sezioni del dominio si e' anche passati ad un filtraggio del pacchetti.

Il router da cui si dipende, infatti, vieta connessioni con IP al di fuori di 194.20.32.1, 195.31.190.135, 195.31.190.63 e che non siano sulla porta 80.

Tuttavia c'e' una nota : dalla tabella di routing di uno degli ascend tutto il dominio 195.31.190.XXX sarebbe visibile ma cio' non passa sopra il controllo della porta che, comunque, e' abbinato anche all'IP..... quindi pacchetti TCP/IP con header contenente IP e porte ben precise."

Per scoprire i green è utile usare i wardialers, altresì detti scanner, che sono software che automaticamente compongono numeri di telefono e vedono cosa risponde, cioè se risponde un computer o meno.

Usare i green è rischioso perché si provoca un danno economico alle ditte che li hanno messi su, e che quindi nel caso vi sgamassero ve la faranno pagare cara (galera, multa e sequestro di PC).

3.3.2 Green e Terminal Server

di Fab

Tutte le seguenti informazioni sono solo a scopo educativo, tali informazioni sono solo frutto di voci o di esperienze personali che non hanno portato alla violazione di nessun codice previsto dalla Legge Italiana.

Ultimamente molti avranno notato una corsa ai numeri verdi, i cosiddetti green, da parte di persone stufe di pagare mamma telecom.

Dopo varie scansioni effettuate da persone e' venuto alla luce che molti provider avevano delle loro macchine collegate a tali numeri mentre su altri rispondevano dei Terminal Server dove, a volte, non vi era nessun controllo.

Non posso dire nel dettaglio quali sono questi numeri ne quali sono i vari provider o computer che li usano; posso solamente fare alcuni nomi in quanto numeri pubblicizzati dai provider stessi o non piu' utilizzabili.

Come ho gia' detto in una mia email e come hanno fatto gia' altri prima di me un numero verde che aveva fatto storia era il 167012837 ovvero il numero verde usato dalla Tin per fare le attivazioni.

Facendo tale numero ed aprendo la finestra terminale (si puo' fare anche ora) si notera' che senza alcun controllo di sicurezza si entra in un terminal server, in questo caso un ascend.

Tali macchine gestiscono l'assegnazione del IP via ppp e sono macchine dedicate a gestire i vari modem ad essi collegati e i vari chiamanti. Vi sono vari comandi (molto simili a quelli dei cisco) che, in parte, si possono ottenere scrivendo help o ? e poi dando invio.

Per vedere se una macchina di questo tipo e' in rete basta provare a fare un telnet o pingare una qualche macchina e vedere se risponde. I comandi telnet e ping sono dediti a fare cio'.

Se cio' non funzionasse le speranze non sono finite. Come succedette al 167012837 qualche dipendente telecom mise un server proxy su una macchina fuori dal dominio dell'ascend e utilizzo una macchina in rete (

non l'ascend) per vederla.

Come tutte sapete (spero) 194.20.32.1 e' la macchina dove sono le prime pagine che gestiscono le iscrizioni (le altre sono su 195.31.190.63);

proprio questa macchina era usata come gateway per vederne un'altra (195.31.190.135) dove giaceva un server proxy ftp e http sulla porta (classica) 8080.

L'unico modo per accorgersi di questa macchina era facendo uno showdella tabella di routing; il comando show ip routes fa questo.

Un controllo dell'arp non sarebbe servito a questo scopo mentre e'stato molto utile per individuare gli IP delle macchine collegate che stavano lavorando.

Dovete sapere che per molto tempo diverse persone montavano server irc, ftp e usavano la sottorete di

cui faceva capo l'ascend per chiaccherare e scambiarsi files.

Da un calcolo aprossimato oserei dire che 200 persone diverse hanno usato tale servizio tra il Dicembre 97

e il Marzo 98 per un totale di 2 Giga di trasferimenti cadauna.

Un altro numero che e' stato usato per un po' di tempo e che ha dava connessioni complete ad internet era il numero verde gestito dall'USL del Veneto.

A tale numero rispondeva un Cisco il quale (dopo i controlli per vedere se era in internet detti prima) permetteva di girare su internet senza problemi.

Dopo una settimana queste persone inserirono il sistema di autentificazione PAP sul ppp ma tale controllo si poteva raggirare usando il buon vecchio protocollo SLIP, lasciato abilitato e senza nessuna forma di sicurezza.

Vi sono molte altre macchine collegate a numeri verdi, da provider a macchine del governo ma sono quasi tutte coperte da sistemi di sicurezza che richiedono a chi le voglia utilizzare una login (o Username) ed una passwd.

Famosi provider italiani come MDnet vendono abbonamenti su numeri verdi ormai gia' da molto anni, altri (

senza dirlo a nessuno) hanno gia' diversi numeri attivi.

Un solo consiglio : tali numeri sono pubblici e quindi tutti li possono chiamare sia che siano sull' elenco sia che non ci siano. La violazione del sistema di sicurezza e' un reato molto grave e ne sanno qualcosa quelli che, fino a poco tempo fa, utilizzavano un numero verde a cui faceva capo ItaliaOnLine..... utilizzando comuni account di IOL si poteva accedere alla rete. 3 settimane fa sono scattate circa 200 denuncie sul territorio italiano con 200 altrettanti processi.

Pensateci bene, quindi, e valutate il tutto.

I numeri che ho citato non sono piu' utilizzabili agli scopi prima citati e gli ho citati liberamente poiche' nessun reato era stato commesso durante il loro utilizzo.

Potrei darvi anche gli estremi di una delle leggi piu' significative del codice penale riguardante i crimini informatici ma mi limitero' a citarne solo alcune righe (cio' potrebbe esservi di aiuto) :

"...In caso di semplice immissione non autorizzata si rischia la reclusione fino a tre anni.....per misure di sicurezza si intendono tutti i mezzi di protezione logici e fisici (password, chiavi, ...) che dimostrino la volonta' del soggetto, che gestisce il sistema

informatico o telematico, di voler espressamente riservare l'accesso e la permanenza nel sistema alle sole persone da lui autorizzate"

3.3.3 Grabba la pass del tuo ‘amico’

di CDP

Una attività che sta a metà tra il Phreaking e l'Hacking è quella di cercare di scroccare il collegamento ad internet.

Per cercare di trovare la password usata da una persona che conosciamo dobbiamo cercare di sapere il più possibile di lui.

Il login lo apprendiamo quasi sempre dal suo indirizzo di posta elettronica, per la pass un metodo è tirare ad indovinare, visto che di solito si usa il nome dell'amata, del cane, del calciatore preferito o pilota di F1, il proprio numero di targa, il qrz se si è un radioamatore, il numero di telefono e via dicendo. Compilando una lista di possibilità si può trovare la password nel giro di un paio di settimane, ma non sempre è così facile.

Cosa fare allora, oltre che pregare? Beh se siete fortunati come me e il vostro amico capisce poco o niente di computer siete quasi a cavallo...

Mettiamo caso che il vostro amico vi chiami perchè ha un problema col computer o col modem (che magari potete causargli proprio voi... tanto si fida, basta essere sufficientemente bastardi!;) e vi chiami per risolverlo, allora voi userete un programmino ad hoc che chiederà al vostro amico di inserire username e password e ve lo memorizzerà in un file che consulterete a casa con comodo! Facile, no? Vi assicuro che funziona, io l'ho già fatto con successo!!

Ma esiste anche roba migliore in giro! Programmi TSR invisibili che registrano tutto ciò che viene scritto con la tastiera! Phreak it out! (e andate a scaricarvi da Spaghetti Phreakers, naturalmente…)

3.3.4 Internet cafè

di BrEdDoLo

Curiosi???? Non credo..... è una di delle bastardate che si fanno più facilmente, cmq ve ne parlerò lo stesso

.... Quest'estate mi trovavo in calabria in un villaggio turistico... per la prima settimana mi sono veramente divertito ma sentivo che mancava qualcosa e così guarda un po' ho trovato due postazioni Internet Cafè con l'inespugnabile sistema a carte magnetiche!!!! caxxata tremenda..... sembrava fatto veramente bene: 1) Il tasto F8 della tastiera per il menu di avvio era praticamente spiaccicato :(((

2) win95 partiva in esecuzione automatica co sto programma NetCard2 (favoloso lo consiglierò a molti!!!!) 3) L'unica cosa che si poteva fare era ridurre a icona la finestra de sto programmino... e trovarsi poi di fronte lo schermo verde di win95 completamente vergine!!! :((

4) CTRL+ALT+CANC era inutile!!!

Al chè mi sono detto caxxo possibile che il buggatissimo win95 mi inculi così?....

unguèèè non sono il tipo che paga 20 carte per connettersi!!! (in Calabria costa così..:( )

noooooooooo, i cari tecnici si erano dimenticati di un altro tastino magico: F3 eheh così per puro caso mi sono trovato di fronte alla finestrina trova file!..... ma non era finita qui... non appariva nulla....nisba nadaaaaaa... niente hd niente floppy... la cosa mi sembrava alquanto stranetta ma poi un mitico lampo di genio!!!! Era impostato su visualizza file (nessun tipo) AH AH AH caxxo a ste cose ce se devo pensare prima! fatto questo l'unica preoccupazione era disabilitare netcard, cosa che avrebbe riabilitato tutte (o quasi) le funzioni di windowz...mi fa schifo solo nominarlo....)

Entro nella directoruzza e trovo grosso come una casa: DISABILITA.EXE !!!! Eh ma allora ditelo eh! clikkko una prima volta e niente... clikko la seconda e te pareva funza benizzimooooooooooooo.... windowssss era miooooooo....

bhè poi il resto è normale amministrazione .... telefonatina interurbana al proprio provider.... (tanto paga il villaggio ahahahaha)...e navigatuzza per circa tre orette filate!!!!!!!!!!!

3.4 Piccola truffa col trasferimento di chiamata

di Chaos Engine

Questa e' una truffa perfetta.

Prima di tutto bisogna spiegare in cosa consiste il trasferimento di chiamata: ogni abbonato Telecom ha la possibilita' di fare in modo che ogni telefonata diretta al suo apparecchio venga dirottata su un altro.

(ES. Io telefono a casa di un amico che pero' ha deciso di trasferire le chiamate nella sua casa in campagna, dove si e' trasferito lui, e il telefono suona non dove io ho chiamato ma nella casa in campagna dell'amico).

Questo servizio ha un risvolto molto piacevole: io pago la telefonata da casa mia a casa dell'amico e lui paga la tratta da casa sua alla casa in campagna.

Ora la truffa consiste nel riuscire ad impostare il trasferimanto di chiamata su un apparecchio non vostro in modo che ridiriga le chimate dove garba a voi: per farlo e' sufficiente comporre un numero da

quell'apparecchio e poi seguire le istruzioni della voce preregistrata (in due minuti avete finito).

Non e' facilissimo, e' vero, ma se dovete tenere dei collegamenti costanti con l'estero, potreste trovarvi tra le mani bollette stratosferiche, che potete scaricare nelle tasche del malcapitato!

Potreste riuscire a chiamare negli states o a servizi telefonici a pagamento (166, eccetera) spendendo la normale tariffa urbana! Questo giochetto e' fattibile ad esempio nei luoghi pubblici, dove di solito si usa il telefono del posto e poi si pagano gli scatti al banco: impostate il vostro trasferimento e poi andatevene in una cabina e fregateli.

State accorti e non fate i sacripanti: se trasferite le chiamate verso un numero privato, non sfruttate il

"servizio" piu' di 1 - 2 volte! Vi potrebbero beccare!

Appendice di CDP: Se casomai la vostra vittima non dovesse avere il trasferimento di chiamata attivato, attivateglielo voi!!! Basta scrivere a suo nome (o telefonare) e il gioco è fatto.

3.5 Telefono col lucchetto? No problem!

di CDP

Ok ragazzi, questa è una tecnica vecchissima, ma potrebbe esserci qualcuno di voi che ancora non la conosce (seee.. ma dai!).

E' la prima cosa che un vero piccolo phreaker scopre (Anche Joe Engressia ha cominciato così): è possibile comporre i numeri telefonici senza usare la tastiera del telefono, utile quando ci si trova alle prese con un telefono al quale qualche taccagno ha messo un lucchetto o qualcosa di simile.

Per ottenere i numeri bisogna premere leggermente la levetta sulla

quale si poggia la cornetta. Bisogna premerla fino in fondo e bisogna

lasciarla subito. Ad ogni numero corrisponde un numero di pressioni

della levetta... lo schema è semplice ma ve lo scrivo lo stesso:

1 .

2 ..

3 ...

4 ....

5 .....

6 ......

7 ....

8 ....

9 ....

0 ....

ogni . corrisponde ad una pressione.

Un ulteriore metodo consiste nel ’avere con se uno di quei tastierini per comandare le segreterie telefoniche a distanza.

3.6 La Magica Blue Box

di CDP

La blue box è stato forse il più grande mito della storia del Phreaking. Un magico apparecchietto che permetteva non solo di chiamare gratis ogni angolo del mondo, ma permetteva a chi ne avesse le capacità, di comandare tutto il sistema telefonico del ’era pre-ESS in America. Le blueboxes furono usate con successo anche in Italia, nella golden era del Phreaking (primi anni 90), anche se in questo caso erano blue box software.

Il funzionamento della blue box era semplice:

I collegamenti telefonici sulle lunghe distanze erano costituiti dai cosidetti trunks, che collegavano le varie centrali telefoniche. Su questi trunksviaggiava sempre, quando non venivano usati, una frequenza (2600hz per l'America) che per le estremità dei trunks stava un po’ a significare: nessuno mi sta usando, sono libero.

Il phreaker telefonava ad un numero verde, per il cui collegamento veniva immesso su un trunk. La centrale telefonica registrava che aveva chiamato un green e non iniziava nessun addebbito per la chiamata. Sul trunk non veniva più eseguito il 2600. Il telefono squillava.

A questo punto il phreaker suonava, tramite la blue box, il tono 2600 nella cornetta. L’estremità del trunk a cui faceva capo il green, pensava che l’utente avesse deciso di attaccare e si sconnetteva (poiché sentiva il 2600 sul trunk). Ma l’estremità su cui si trovava il phreaker continuava a pensare che il tizio stesse telefonando al green. Il phreaker ora aveva il trunk a sua disposizione e poteva, tramite l’uso di altri toni (i famosi kp & co.) indirizzare la chiamata su un numero a piacere… tanto per la centrale lui stava parlando con un numero verde e quindi non gli veniva addebitato nulla!

Purtroppo però tutto ciò non è più possibile da quando è stato modificato il sistema telefonico in America, in Italia e un po’ in tutto il mondo.

Ed ora un po’ di storia: (Passo tratto da Butchered from Inside)

"Il blue box era nato da una scoperta fatta da un tecnico di trasmissioni radio il cui nome e' John Draper. Egli aveva notato che attraverso un fischietto trovato in una scatola di cereali era possibile fare chiamate senza pagare niente. Ok molti di voi possono pensare che egli si sia fatto una canna e poi, preso dalle allucinazioni, si sia messo a fischiare sulla cornetta, in realta' lo pensavo anch'io, ma non e' cosi'. Infatti egli si era accorto che quel fischietto emulava una frequenza di 2600hz che guarda caso era proprio quella che in gergo telefonico viene chiamata TRUNK CODE o semplicemente TRUNK.

Ben presto il suo nome fu associato alla scatola di cereali e venne chiamato CAPITAN CRUNCH. Comuque alla stessa scoperta erano arrivati anche molti altri ragazzi, per lo più ciechi. Joe Engressia al ’età di soli 8

anni riuscì a ‘seizeare’ un trunk fischiettando nella cornetta mentre ascoltava una registrazione di un numero verde, chiaramente non si rese conto subito di ciò che aveva scoperto. Captain Crunch rimane però quello che che ha esasperato la tecnica, la leggenda vuole che si sia costruito una switching board sofisticatissima e che viaggiasse in un camper attaccandosi al e cabine del telefono…

Draper è uno dei migliori hacker (oltre al primo phreaker) che ci sia mai stato.

Egli e' stato arrestato un paio di volte e, per non essere trattato come una ragazza dai detenuti, ha confessato di aver svelato molti dei segreti che lui conosceva a quei criminali, e oggi egli teme che gran parte di questi siano dietro alle piu' grosse organizzazioni mafiose.

Come se non bastasse Draper, che ha fondato un ditta che si occupa della creazione di pagine web, riceve continuamente visite da parte dell'fbi la quale gli sequestra tutto bloccando il suo lavoro per mesi e facendogli perdere un sacco di clienti, questo solo per controlli ... "

Non e' piu' possibile oggi utilizzare le blue boxes nemmeno qui in Italia.

Tutto questo lo dobbiamo al fatto che la Telecom (sempre grazie all'At&t), ha introdotto quello che si chiama Electronic

Switching System e che attraverso il CCIS filtra il trunk non permettendo quindi il suo passaggio. Attenzione pero' cambiare l'intera rete telefonica non e' una cosa che si fa in un giorno, ecco perche' probabilmente in alcune parti d'Italia il blue box e' ancora possibile.

Quello che poi non mi convince molto e' che in realta' non so come si comporta il CCIS ad altri TRUNK e quindi forse il blue boxing verso paesi del terzo mondo si puo' fare.

Per scrupolo eccovi le frequenze (Estrapolate da Butchered from Inside):

FOR CALLING VIA: FREQUENCIES:

ALGERIA 2000 Hz

ARGENTINA 3825 Hz

AUSTRALIA 600& 750 Hz

(SEPERATE)

AUSTRIA 2280 Hz

BAHAMAS 2600 Hz

BANGLADESH 3825 Hz

BRAZIL 3825 Hz

BURUNDI 3825 Hz

CAMEROON 3825 Hz

CANADA 2600 Hz

CHILE 3825 Hz

CUBA 2100/3825 Hz

CYPRUS 3825 Hz

CZECHOSLOVAKIA 2280 Hz

DENMARK 3000/3825 Hz

DOMINICAN REP. 2600 Hz

FIJI 3825 Hz

FRANCE 2280/3850 Hz

GHANA 3825 Hz

HUNGARY 2280/3825 Hz

INDIA 2400 Hz

IRAQ 3825 Hz

(ONLY, WHEN YOU FIND A NUMBER AFTER

THE GULF-WAR IN 1991 - HAHA!)

IRELAND 2040/2400 Hz

COMPOUND 2280 Hz

ISRAEL 3850 Hz

ITALY 2040/2400 Hz

COMPOUND & SEPERATE

che si basano sull'utilizzo dell'ESS e di event

JAMAICA 2600 Hz

JORDAN 3825 Hz

KENIA 2040/2400 Hz

KOREA 3825 Hz

LIBERIA 3825 Hz

LUXEMBOURG 3825 Hz

MADAGASCAR 2280 Hz

MOROCCO 2280 Hz

MOZAMBIQUE 2400 Hz

500/ 20 Hz

1625 Hz

3350 Hz

3825 Hz

NIPPON 2600 Hz

NORWAY 2400 Hz

NEW ZEALAND 600/ 750 Hz

2280 Hz

OMAN 3825 Hz

PERU SOME DIFFERENT FREQUENCIES!

PHILIPINES 3825 Hz

OLD: 2600 Hz

POLAND 2280 Hz

3825 Hz

500/ 20 Hz

2100 Hz

PORTUGAL 3825 Hz

ROMANA 3825 Hz OR 2280 Hz

SOUTH AFRICA 600/ 750 Hz

SEPERATE 2280 Hz

SPAIN 2500 Hz

SURINAM 3825 Hz

SWEDEN 2400 Hz

SWITZERLAND 3000 Hz

SYRIA 3825 Hz

TANZANIA 3825 Hz

THAILAND 2400 Hz

UGANDA 2040/2400 Hz

UNITED KINGDOM 600/ 750 Hz

SEPERATE 2280 HZ

USA 2600 Hz

USSR 1200/1600 Hz SEPERATE & COMPOUND 2600 Hz

YUGOSLAVIA 2280 Hz

ZAMBIA 3825 Hz

3.7 Vampirare i Cordless

di CDP ed ellegi

Ok, questo metodo non è nuovissimo ma mi è venuto in mente solo l'altra sera su IRC.

Innanzitutto per poterlo attuare avete bisogno di un cordless di tipo vecchio, cioè senza codici o canali, che insomma non comunichi dati alla sua base. Inoltre dovrete essere in una zona dove ci siano altri cordless...

sennò a chi vi attaccate??

Il passo successivo è spegnere la base, accendere il cordless e vedere se avete il segnale o se potete ascoltare delle voci, se sì siete a cavallo!

Se poi siete perfezionisti potete cambiare l'antenna del cordless con una più potente. Svitate l'antennina, saldate un cavo coassiale sul circuito e collegatene l'altra estremità ad un'antenna tarata sui 45 Mhz. La lunghezza del cavo deve essere di 1,6 metri o multipli e sottomultipli.

Vi ricordo che con questo metodo non danneggiate la telecom ma solo il poveretto proprietario del cordless a cui vi attaccate. Quindi a meno che non lo odiate a morte lasciate stare.

3.8 Calling Cards

di Timescape

Le calling cards piu' usate sono solitamente quelledi :

AT&T (American Telephone & Telegraph)

MCI (adesso Worldphone)

US SPRINT (adesso GLOBAL ONE).

Dall'Italia i numeri gratuiti per accedere ai centralini automatici delle suddette sono :

AT&T (1721-011)

MCI (1721-022)

US SPRINT (1721-877)

tutte e tre i servizi richiedono l'inserimento del numero da chiamare (che per at&t e mci puo'

essere o un numero statunitense nella forma acn-phone (es: 617-258-7111) o un numero internazionale nella forma 011-cc-phone o 00-cc-phone (es:011-39-2-4040401, 00-39-2-4040401 Milano) e della calling card (che per tutte e tre le compagnie e' di 14 cifre XXX-XXX-XXXX-XXXX).

Nella golden age italiana (prima del '93) erano usatissime le AT&T CC, con il solo problema che all'epoca i sistemi automatici non c'erano e dovevi parlare in americano stretto con una operatrice (frase divenuta famosa : AT&T, May I Help you ? per MCI : MCI upreader 543, How can I Help you ?, chissa' se saranno rimaste uguali (nel senso che le frasi di risposta sono definite dalla politica aziendale) e che non potevi chiamare al di fuori degli USA.. a meno di non chiamare con la CC un PBX o PABX in USA e da quello richiamare dove volevi anche le Allied Teleconferencing col quale si facevano conference notturne in 7-8 di durata oceanica...

(10288-0700-456-1000 il numero dell'alliance se mi ricordo bene e se non e' variato..)

Vi anticipo che NON esistono algoritmi per calcolare le AT&T CC.. le private sono composte dal numero dell'abbonato + 4 cifre di codice rilasciate a caso da un calcolatore at&t .. le aziendali sono composte da 10

cifre algoritmiche (l'algo e' sconosciuto) + 4 a caso... Vi lascio per la storia la piu' bella at&t che abbia mai visto.. l'avevamo solo in due e duro' 30 giorni (la media di funzionamento prima che una carta venisse bloccata era di 2-3 giorni nel 1992):

212-433-5421-6214

3.9 Giocare via modem gratis e altro

di CDP

Allora, premetto che questo metodo non l'ho provato ma dovrebbe funzionare al 100%.

Avete presente quei numeri verdi ai quali è possibile telefonare per sottoscrivere un abbonamento a TIN e ci si naviga come si fosse in Internet (anche se si rimane sempre sul server?). Ebbene quando vi collegate vi viene dato un indirizzo IP...

Quindi se un vostro amico si collega allo stesso numero e stesso server può collegarsi con voi tramite il vostro indirizzo IP!

Potrete così giocare a tutti i giochi che supportano il multiolayer via internet!!

Il problema semmai è come dare il proprio IP agli amici, che sò fate voi... piccioni viaggiatori, CB, telefonino... sbizzarritevi!

Se volete provare subito vi dò questo green:

167012837

(Questo è quello che trovate alla risposta di Internet gratis, seguendo quel metodo ne potreste trovare altri) Vi ci collegate con accesso remoto e alla schermata del terminale (a connessione effettuata) digitate: ppp d

e vi viene dato un IP address.

Se non avete voglia di giocare potete lanciare il browser e collegarvi a www.tin.it e farvi quattro risate.

Sezione 4: Telefonia cellulare.

4.1 Introduzione

di CDP

Il settore del cellular phreaking è sicuramente uno dei più evoluti e yuno di quelli che hanno fatto girare più soldi tra i truffatori. Sfortunatamente chi scopre nuove cose è colui che lo fa per lucro e le informazioni sono difficilissime da scoprire. Noi di Spaghetti andiamo cercando da tempo qualcuno che sia parecchio esperto nel settore per aiutarci a sviluppare questa sezione.

4.2 Cellulari e clonazione Etacs

Estratto da Butchered From Inside n° 2

In coerenza con lo stile di pIGpEN e per mancanza di idee :)

Autore: |PazzO|

Consumo: 20 ore di sonno + o -, 3 cellulari bruciati (scherzo), 1 rotolo di carta igienica (raffreddore)

Rompimenti di coglioni: 2 Telefonate, Citofono, Cellulare, Mia madre, mia sorella!! GRRRRRRRRR

Musica Ascoltata: (accendo la radio e scrivo a caso) OasiS a manetta!!!!

Dedica: A Micaela perche' anche se non la conosco (ma chi e' questa tizia lo sapro' mai?) ha un server talmente impenetrabile che sta facendo uscire pazzi tutti gli hackers (o lovers) di S0ftPj

Subject: Cellulari and related (Almeno questo era l'intento prima di scrivere l'articolo)

Parte: Prima e Seconda

Premetto che se non ve ne fotte un caxxo di come funzionano i cellulari, di cosa sono e perche' ci sono 3 diversi sistemi, di cosa usate per telefonare e di come lo fate, ma vi interessa solo chiamare gratis allora o siete dei Lamah o siete degli impazienti di quelli che aprono 300 finestre di NETscape fino a fare impallare tutto come me, in quest'ultimo caso jumpate direttamente alla seconda parte dell'articolo, anche se vi consiglio di leggerlo attentamente perche' e' molto interessante (almeno credo).

La domanda che in generale affolla la mente di tutti i Phreakers d'Italia, ma soprattutto la mente dei miei quando pagano la bolletta del telefono e' "Ma si puo' telefonare gratis in qualche modo tipo alzo la cornetta sto 4 ore

attakkato e non pago un caxxo????".

Beh vi anticipo che alla fine del mio piccolo/grande articolo voi riuscirete tranquillamente a chiamare gratis* ovunque voi crediate. *(per il significato del termine Gratis vai piu' avanti).

Voglio premettere che tutto cio' che scrivo e' a scopo PURAMENTE INFORMATIVO ED EDUCATIVO e che e' proibito dalla legge del nostro stato manipolare telefoni cellulari a danno altrui o della Telecom Italia Mobile per trarne vantaggi. Non sono dunque responsabile per atti criminali dovuti al cattivo uso di queste informazioni e non mi ritengo nemmeno responsabile per danni causati a telefoni cellulari E-Tacs o GSM dal cattivo funzionamento di codici o altro contenuto in questo articolo. Non prendetevela con me quindi se il vostro cellulare smette di funzionare o fonde inspiegabilmente, anche perche' e' molto difficile per un inesperto manipolare il Firmware di un telefono non compromettendolo definitivamente. Ah, dimenticavo, se vi arrestano per aver clonato 1,10,100 cellulari io non rispondo delle vostre azioni criminali.

Questo articolo e' scritto per i possessori di cellulari in modo da consentire di proteggersi da eventuali clonatori.

Innanzi tutto devo fare una precisazione sul termine Gratis. Molti intendono per telefonare gratis il telefonare senza pagare una lira, beh sarete sorpresi dal fatto che non e' cosi'. Esiste una sottile differenza tra il chiamare gratis e il chiamare a spese altrui. Nel primo caso la mia chiamata non la paga nessuno poiche' non viene addebbitata dalla TIM, mentre nel secondo caso la mia chiamata viene addebbitata a un povero disgraziato al quale avremo clonato la sim o il cellulare, quindi state attenti poiche' queste info in campo di Cell Ph oggi permettono solo di telefonare a spese altrui e non gratis, ma penso che

per voi non faccia poi grande differenza. ;-))

Iniziamo ora la parte veramente interessante con dei cenni preliminari sui sistemi cellulari oggi in uso.

Esistono due sistemi di cellulari attualmente in uso in Italia e un terzo in uso nel mondo intero, cioe' un sistema analogico e due sistemi digitali.

Il primo, in Italia, e' definito sistema E-TACS ed e' attualmente quello che garantisce la maggior copertura sul territorio nazionale sia a livello di linee disponibili sia a livello di antenne impiantate.

Il sistema E-tacs si basa su una tecnologia di prima generazione ovvero analogica. Il cellulare agganciato alla rete infatti non tramuta le informazioni in formato digitale ma le trasmette cosi' come le riceve dal microfono o dalla tastiera all'antenna che le smista alla centrale sino alla rete Telecom.

Questo sistema antiquato ci permette oggi di ascoltare con un semplice scanner le conversazioni altrui senza poter essere scoperti da nessuno e senza disturbare o interrompere la linea (per freqs e info vedi: BFI n.1 "Radioascolto per veri ascoltoni",Vanadio).

In pratica il cellulare possiede un numero di identificazione che viene fatto coincidere con il Serial Number, grazie al quale si registra sull'antenna che inoltra la chiamata. In pratica quando noi premiamo il tasto invio del nostro telefono esso dialoga per 2-3 secondi con l'antenna che lo sta servendo, trasmettendogli il suo numero di identificazione associato al numero del chiamante; intanto l'antenna dialoga (questa volta via cavo) con la centrale telefonica, la quale controlla se l'utente e' abilitato a chiamare -del tipo: se ha pagato la bolletta- ;-)

E dopo aver ricevuto la conferma attende che il cellulare le trasmetta il numero da chiamare, il cellulare ricevuto l'ok trasmette il numero e si connette alla rete telefonica ed effettua la chiamata (voglio ricordare che la prima parte del processo si ripete ogni volta che il cellulare passa da ricerca campo a campo per consentire la ricezione delle chiamate con un grande dispendio di energia).

E allora come faccio a fottere questo sistema?

Bisogna dire che i cellulari nascono di fabbrica senza nessun contratto o registrazione ma gia' con un numero seriale: e chi li attiva?

Ma i nostri amiconi della Telecom, naturalmente, che posseggono tutti i codici di riprogrammazione di telefoni cellulari e che prendono per fare questo L.500.000 di attivazione (mocc a'loro).

Ma se lo fanno loro che sono stati assunti per raccomandazioni e che non distinguono un pc da un televisore, perche' io non dovrei farlo?

L'unico modo per fregare quindi l'antenna (che io sappia) e' simulare che il nostro cellulare sia un untente abilitato e per fare questo bisogna inserire il codice ed il numero di qualcun altro. Su questo torneremo dopo... (ehehe sono sadico!!)

Il sistema E-tacs si e' rivelato di scarsa sicurezza e bassa qualita' facilitando l'introduzione del nuovo standard europeo per la telefonia digitale che e' rappresentato dal GSM ovvero Global Mobile System.

Il passaggio dall'analogico al digitale e' dunque tutt'ora in corso e si completera' entro il 2000. Ma le differenze tra analogico e digitale quali sono dunque? Beh a tutti quelli che mi fanno questa domanda io faccio questo esempio: pensate ad un giradischi vecchio modello e ad un lettore cd, il primo

legge dai dischi direttamente la musica incisa e ha il compito di amplificarla tramite la testina che trasforma le incisioni in suono e tramite l'amplificatore, il secondo invece ha il compito di trasformare le informazioni COMPRESSE nel formato digitale in suoni e poi di amplificarle garantendo quindi il passaggio di informazioni di qualita' maggiore in un minor spazio e in formato digitale.

Oggi il sistema digitale consente una sicurezza maggiore grazie al sistema nuovo di autenticazione (del quale parlero' dopo), un risparmio di energia grazie alla nuova tecnologia dei cellulari, una qualita' quasi perfetta di trasmissione (almeno in teoria) grazie al flusso di dati, la possibilita' di utilizzare piu' apparecchi con lo stesso codice sfruttando la mobilita' della SIM CARD (il cuore del telefono) e infine il nuovo servizio di roaming per collegarsi sulle reti di piu' gestori sparsi sul Globo. Piu' propriamente il sistema GSM e' nato per la trasmissine DATI applicata alla telefonia, quindi per quanto possa sembrare paradossale la funzione di trasferimento dati audio (Telefono) e' da considerarsi una funzione accessoria di quello che e' il piu' potente sistema di trasmissione dati via etere al mondo.

Ma come funziona in pratica il sistema GSM?

Il sistema Gsm si basa sulla trasmissione dati su una determinata frequenza radio assegnata dal governo al Gestore (colui il quale si prende l'onere di costruire le antenne e di vendere l'abbonamento a prezzi concorrenziali -vedi TIM o OMNITEL-). L'apparecchio GSM oggi disponibile in numerose Marche, modelli, dimensioni e capacita' diventa quindi Universale grazie alla SIMcard, che e' la tessera che contiene le informazioni relative al contratto dell'abbonato (algoritmo di idefinticazione) e dati relativi alle impostazioni

del cellulare, numero di telefono etc (Seguira' presto una DETTAGLIATA spiegazione del funzionamento della SIM CARD e della sua composizione FONDAMENTALE per poter riprodurne una"in casa").
Il sistema GSM e' inpenetrabile in fase di "identificazione" con l'antenna grazie all'algoritmo di identificazione che viene assegnato al Gestore il quale a sua volta lo usa per produrre le proprie schede SIM. Quando noi premiamo il tasto invio, questa volta il cellulare attende la trasmissione di un numero casuale a 128 bit che gli verra' fornito dal centro autenticazione contattato dall'antenna, il numero passa dal cellulare alla sim che lo passa attraverso le sue copie degli algoritmi A1,A8 e ki, formula la Risposta a 32 bit e la restituisce al network, lo stesso numero casuale viene di nuovo manipolato dall'algoritmo A8 e dal ki e forma la cyper key (la chiave) che viene inviata al network, il sistema di autenticazione controlla se le due chiavi sono state trattate con l'algoritmo A8 e ne estrae il ki (identificazione) controllandone la validita' e dando quindi il via libera alla transazione.
Questo sistema garantisce che anche con la completa intercettazione dei dati non si possa risalire a nessuna informazione utile ai fini del Sim cloning.
(Che ne dite e' sicuro o no questo sistema?)
Il Gsm quindi e' un sistema sicuro (o almeno questo si crede ;-), ma poi daremo un'okkiata a come riuscire a "fottere" questo sitema.
Il terzo e ultimo sistema (che io conosca) e' il global satellitar system che adopera la tecnologia digitale utilizzando pero' come antenne di diffusione non le classiche celle ma i satelliti in orbita intorno al globo, garantendo una copertura TOTALE dell'intera terra, ma con costi altissimi di gestione e quindi di servizio. Non mi sono interessato granche' di questo servizio e non so fino

a che punto ne valga la pena oggi visto che esistono pochissimi apparecchi in giro in grado di captare i segnali del satellite e quindi di usufruirne (esclusi i telefoni degli Aereoplani), ma comunque fregare questo sistema e' piu' facile di quanto si pensi (dopo vi svelero' il mio piccolo segreto!!).

Fine della prima parte...

SECONDA PARTE (cercate di chiudere qualche finestra del browser prima ;-)

Se avete chiuso tutto le finestre e vi siete un po' tranquillizzati iniziamo con la seconda parte che tratta di E-Tacs Cloning. Ho gia' detto prima che non e' possibile clonare un qualsiasi cellulare E-Tacs poiche' non possediamo l'algo (penso) che genera i Serial Number ai produttori di cellulari i quali poi li notificano alla Telecom.

Di conseguenza per poter clonarne uno dovrete possedere almeno un serial number di un cellulare ATTIVO (cioe' che ha un contratto o una Tim card ricaricabile ATTIVA) e il numero di telefono di quel cellulare. In pratica tutto quello che dovete fare e' prendere un cellulare, sollevare la batteria, leggere il Serial Number che in genere e' accompagnato da un codice a barre, leggere il modello preciso del cellulare e infine appuntarsi anche il numero di telefono di quel cellulare.

Fatto questo, che e' la parte piu' difficile di tutto il processo ed e' anche quella che puo' causare piu' problemi dal punto di vista legale se non usate un vostro cellulare per questo esperimento, siete gia' al 50% del lavoro.

I modelli di cellulari esistenti oggi sul mercato sono moltissimi e non posso elencarli tutti, quindi partiro' dai modelli piu' diffusi, in particolare con il modello Ericsson EH237 che e' stao il primo cellulare che io abbia mai clonato.

Ora chiudetevi in una stanza soli, lontano da occhi indiscreti, portetevi una bella ragazza con voi (anche se non garantisco la riuscita del cloning in queste circostanze), oppure andate in Metropolitana o in P.zza Duomo a Milano, tanto nessuno notera' niente, e iniziate ad entrare nel "test mode" del vostro cellulare, cosi' potrete esplorare le funzioni nascoste e le opzioni impostate dal gestore telefonico della vostra zona.

Per riuscire a modificare il software di un cellulare (il quale poi non e' nient'altro che una aaprom riprogrammabile) in alcuni casi basta possedere i codici di riprogrammazione, mentre in altri casi bisogna "costruire" un cavo per interfacciare il Telefono cellulare con il vostro Personal Computer, dal quale poi lanceremo un programma di programmazione cellulare che variera' da modello a modello, ma che avra' sostanzialmente le stesse funzioni, cioe' riprogrammazione NAM.

Naturalmente il modo piu' semplice per riprogrammare un cellulare e' quello di utilizzare i codici di riprogrammazione segreti, ma spesso (soprattutto grazie ai nuovi sistemi di sicurezza degli stessi) diviene indispensabile costruire un cavo di interfaccia Parallelo-Piede del telefono armati di molta pazienza, cavi di rame, nastro isolante ed un paio di forbici.

Ma rieccoci al nostro EH 237, per iniziare PROCURATEVELO ;-) ma in caso di impossibilita' seguite bene i passaggi che vi proporro'. Innanzitutto spegnete il cellulare, togliete ogni tipo di blocco e riaccendetelo. Subito dopo averlo riacceso digitate il codice di riprogrammazione esatto:

FCN 923885 (or M 923885)

" 924885 "

" 904885 "

" 904005 "

" 904035 "

" 904085 "

FCN 904030 (il quale vi permettera' di clonare il cellulare 3 o 4 volte al massimo, quindi attenzione!!)

FCN 900000 (il quale invece vi chiedera' ben cinque codici PIN per ora sconosciuti).

Nota bene che il codice di riprogrammazione varia di cellulare in cellulare in base al software montato, per non avere problemi vi consiglio di provare prima i codici di riprogrammazione OGNUNO DA SOLO (spegnendo e riaccendendo il cellulare tra un codice ed un altro) UNO DOPO L'ALTRO (cioe' prima fcn 923885 poi se non accade niente fcn 924885 e cosi' via sino ad arrivare alla fine della sequenza) sino a quando non si entrera' nel test secret mode del cellulare.

Una volta inserito il codice si entra nel menu' del test mode che purtroppo varia non solo da modello a modello ma da software a software, per questo non troverete mai nulla di preciso su come sono strutturati i menu', ma potrete fare benissimo affidamento sulle vostre capacita' intuitive. Quello che dovrete fare e' in pratica riprogrammare il MIN ovvero i numero di identificazione (0337etc/0330etc), piu' precisamente entrare nel menu' del MIN, cancellare con il tasto C il vecchio e riscrivere il nuovo, riprogrammare il SN naturalmente con quello che ci siamo procurati, salvare le impostazioni e riavviare il cellulare. Fatto questo il vostro cellulare si dovrebbe comportare adesso come il cellulare che e' stato clonato, quindi dovrebbe squillare quando qualcuno fa quel numero e addebbitare la chiamata su quel numero, naturalmente senza che il

leggittimo proprietario se ne accorga. Le uniche cose a cui dovrete prestare attenzione sono:

1) non rispondere alle chiamate in entrata

2) non abusare del cellulare, perche' se al malcapitato dovesse arrivare una bolletta esuberante egli non solo si farebbe disdire il contratto, ma la Telecom aprirebbe un'indagine utilizzando come indizi i numeri chiamati da quel telefono, con conseguente rapida gattabuia.

E se quei codici non avessero funzionato?

In tal caso useremo il nostro bel Pc per clonare il nostro cellulare dovendo pero' costruire un cavo che colleghi il cellulare alla porta parallela dello stesso PC.

Ecco lo schema del cavo da costruire con relative istruzioni:

Parte bassa del telefono vista con la tastiera verso l'alto:

^ ^ ^

o o o o o o o o o o o o o

21 8 11

Dove 21, 8 e 11 rappresentano i numeri dei pins della "male 25-way d-plug", ovvero porta parallela che connette la vostra stampante al PC, ai quali vanno connessi rispettivamente il terzultimo, il quartultimo e l'ottavo pin del cellulare.

Naturalmente il modo piu' semplice di procurarsi un cavo del genere e' quello di trovare un vecchio caricatore oppure la presa accendisigari della macchina e modificarlo in modo da renderlo utile al nostro scopo, cioe' tagliando la presa accendisigari e collegando i tre cavi come segnato sopra da una parte e alla porta parallela al pin 21, 8 e 11 dall'altra. Per questo e' importante che

il cavo che avrete scelto non sia uno stampato in plastica per quanto riguarda la presa, quelli cioe' che non si ossono modificare se non squagliandoli (come per es. quelli del PC), ma che sia un semplice cavo da telefono cellulare in modo da poter spostare i tre contatti dove ci interessa che siano.
Spero di essere stato abbastanza chiaro a riguardo, cmq sembra molto piu' difficile di quanto non lo sia in realta', ipoteticamente potreste anche prendere 3 cavetti minuscoli e fargli fare contatto a mano sui pin giusti, magari saldandoceli per un attimo, e infirarli nei buchini della presa parallela, ma vi garantisco che il primo metodo e' il piu' efficace.
Fatto questo lanciate il programma sul vostro pc, seguite le istruzioni e sara' facile come fumarsi un caxxone in un campo di Maxxxxana.
Ci sono delle voci in giro che dicono che i telefoni ericsson hanno una sicurezza che li disattiva dopo 40 volte o meno e li rende inutilizzabili.
Beh, io sono arrivato a vedere cellulari Ericsson riprogrammati per piu' di 30 senza problemi, ma non si sa mai.....
State attenti e seguite le mie istruzioni e tutto dovrebbe andare bene, in questo caso vai all'inizio dell'articolo e leggi cosa penso dell'abuso di queste informazioni a danno proprio o altrui.
Nel prossimo numero tenteri' di fare altri 2 o 3 modelli tipo Motorola, Nec e altri, per ora mi interessava spiegarvi + o - di cosa si trattava.
Per i GSM e' tutto un altro discorso, ci arrivero' presto, e' ancora piu' semplice, ma e' un po' teorico.
A presto amici smanettoni di cellulari.
Se ne sapete piu' di me o credete che abbia scritto qualcosa di sbagliato o volete collaborare con me per proseguire la scoperta del digitale contattatemi

all'indirizzo e-mail S0ftPj98@usa.net specificando che il msg e' destinato alla

mia attenzione.

|PazzO| [S0ftPj98]

4.3 La SIM Card

di CDP

Una SIM card è una Smart-card, quindi ha un processore capace di eseguire un algoritmo di criptamento oltre ad avere della memoria. I codici IMSI e KI non lasceranno mai la SIM Card.

Il SIM (Subscriber Identity Modume) contiene:

- Identità Mobile Internazionale dell'utente (IMSI)

- Chiave di identificazione individuale

dell'utente (Ki)

- Algoritmo per la generazione di chiave cifrata (A3),

con Ki e RAND genera una chiave a 64 bit (Kc)

- Algoritmo di Verifica (A3), col Ki e RAND

genera una risposta 'firmata' a 32 bit (SRED)

- Codice PIN utente (1 & 2)

- Codice PUK (1 & 2), detto anche SPIN

- Rubrica dell'utente

- Messaggi SMS salvati

- Lista delle reti preferite

Kc è ustao per criptare i dati tra MS e BS con l'algoritmo A5 che è contenuto nel telefono (può essere regolarmente modificato)

Quando la rete vuole verificare l'utente, un numero casuale a 128 bit (RAND) viene mandato alla SIM.

Inviando il RAND e il Ki nell'algoritmo A£, viene generata la risposta 'firmata' a 32 bit (SRED) che viene reinviata alla rete per la verifica.

Una SIM card deve avere 6 connettori per interfacciarsi ad un GSM.

/----------\ PINOUT: 1: Vcc= 5v

| | 2: Reset

| 4 3 2 1 | 3: Clock

| 8 7 6 5 | 4: NC

| | 5: Gnd (Terra)

| | 6: Programming voltage

| | 7: Data I/O

| | 8: NC

| |

| |

| ISO SIMCARD |

\----------/

Qualche nota sui comandi SIM:

- A0 F2 00 00 19 (Read status) darà F2 + (25 bytes di dati)

1-4 Riservata

5 Identificatore tipo directory (3F= root/7F = altro)

6 Sub-identificatore (00= root / 01= applicazione)

7-12 riservate

13 Numero di byte che seguono (di solito 0C)

14-18 Riservata

19 PIN status (un piccolo nibble mostra il numero di tentativi rimanenti)

20 SPIN (PUK) status (come sopra)

21-25 riservata

il numero di tentativi di default è 3 per il PIN e 10 per il PUK

- A0 20 00 08 (Verify PIN) seguito da un pin di8 digit (1234= 31 32 33 34 FF FF FF FF)

darà:

90 00 Fine normale

6B 00 P1/P2 sbagliato

67 08 P3 Sbagliato

98 08 Contraddizione col PIN Status

98 04 Codice segreto errato

98 40 Codice segreto errato - Istruzione bloccata!

92 0x Aggiornamento avvenuto dopo x tentativi

92 40 Aggiornamento impossibile (EPROM della scheda difettosa)

- A0 A4 (select)

- A0 B0 (Read Binary)

4.4 Funzionamento di un centro ricariche Timmy

DISCLAIMER :

Non sono responsabile, non so niente, non ho visto niente, non mi rompete

i coglioni, non lo ho scritto io etc.....

Ci siamo capiti !!!!! :-)

Allora, eccomi qui ad illustrare il funzionamento dei Centri Tim e piu'

in particolare la questione della ricarica dei Timmy.

I Centri TIM, per poter effettuare tutte le procedure necessarie alla

registrazione dei contratti e alla ricarica, si collegano via Modem ad

un computer centrale della TIM con cui scambiano dati, informazioni,

foto porno ehm, vabbe' ci siamo capiti.

Il collegamento viene effettuato con PC montanti (ah siih... :-)) Windows 3.1

e il software dei nostri sogni: Point of Sale v2.X (dove X e' 3 o 6, la

versione cambia a seconda del menu' in cui siete, penso che questo bug,

chiamiamolo cosi', sia dovuto ad un attacco di pazzia del programmatore),

altrimenti detto anche SID (non conosco il significato della sigla);

parliamo un attimo del collegamento:

- Connessione a 14400

- Connessione di tipo PPP (cosi' riporta il sw di collegamento gia' incluso
nel PoS, sembrerebbe che venga usato anche un driver FTP ma non ci giuro)
- Connessione su un bel green: 167-295XX3 (Vi piacerebbe sapere il numero,
eh, e invece vi lascio come compito a casa, un sano wardialing x trovarlo!)
(Tale numero se non erro dovrebbe avere 2 nodi: Trieste e Roma)
Una volta connessi parte una serie di autenticazioni, che x quanto ho visto
sono strutturate su tre livelli:
1- Autenticazione iniziale (come riportato dal log della connessione del sw
di collegamento col modem) cioe' mi spiego esce 'na roba tipo questa:
ATX3DT167295XX3
Connesso a 14400 LAPCM
VERIFICA DEI DATI DELLA POSTAZIONE IN CORSO
Autenticazione effettuata
Di questa autenticazione non so come possa funzionare, presumo che sia qcosa
a livello o hardware oppure qcosa sull' HD tipo serial (quindi cazzuta).
2- Autenticazione Intermedia: questa avviene a collegamento effettuato gia'
all'interno del sw PoS ed ho scoperto che login e password sono
rispettivamente OPERATORE e TELECOM2 (penso potrebbero andare anche
TELECOM1 o TELECOM, non so, e dovrebbe essere "NON CASE SENSITIVE").
3- Autenticazione finale, o del punto vendita: qui il punto vendita mette
il suo login e pwd ed infatti una volta connessi nel PoS si vede il nome
del negozio.
Per questo motivo quindi si puo' capire che si rischia di inculare il negozio
e non tanto la TIM, anche perche' la ricarica, cosa che interessa
maggiormente, avviene in questo modo:

Il Centro TIM XYZ chiede alla TIM di "caricare" sul suo account x es. 200
ricariche da 50karte, che poi vanno a scalare durante l'utilizzo, quindi
se x es. noi entrassimo con l/p del negozio XYZ gli fottiamo delle ricariche
e inculiamo lui, non la TIM (Se volete fate pure voi disquisizioni del tipo
"il punto vendita non c'entra", "meglio lui che noi, tanto sono pieni di
soldi", "tua mamma e' una X)("!H£"!/)" etc...).
Osservazione MOLTO IMPORTANTE: da quello che ho scoperto posso dire queste
tre cose che rendono un hack molto piu' difficile (come se gia' non lo fosse):
- LE DOPPIE ENTRATE VENGONO SEGNALATE: se qualcuno e' gia' dentro con login
A e pwd B e un altro cerca di entrare con le stesse il terminale segnala
a quest'ultimo che "l'allocazione e' gia' stata effettuata"
(o 'na cosa simile) e quindi non riesce ad entrare.
- LA LINEA NON E' ATTIVA TUTTO IL GIORNO ma viene attivata solo negli orari
di apertura dei negozi quindi scordatevi di collegarvi alle 2 di notte per
evitare la doppia entrata, penso che la disattivino alle 21 (o forse cambia
a seconda del negozio e di quanto sta aperto).
Mi viene inoltre segnalato da un membro del gruppo S0ftProject che:
- LA LINEA NON E' ATTIVA DURANTE TUTTO L'ANNO o forse intende NON FUNZIONA
TUTTI I GIORNI (tipo a Natale penso che non vi permettano di accedere).
Una volta collegati ci si trova in un bel menu' con servizio prepagato,
contratti e tutto quello che volete; la ricarica funziona in modo molto
semplice (non ricordo l'ordine esatto):
- Si inserisce numero di telefono da ricaricare.
- Si inseriscono i dati di chi ricarica (non e' assolutamente necessario
che corrispondano con l'intestatario del numero) cioe' codice fiscale

e se e' gia' presente tra le persone che hanno ricaricato escono gia' i dati

della persona altrimenti vengono chiesti nome, cognome.... vabbe' cque un

lavoro da GenerID v2.2 :-))

-Si sceglie quanto ricaricare

FATTO !!!

P.S.: Non bisogna inserire nessuno codice segreto, PIN, PUK o salcazzo cosa

altro, basta il numero infatti se x caso l'operatore sbaglia e ricarica il

telefono sbagliato, sono solo cazzi dell'utente (non puo' essere neanche

rimborsato ed e' alquanto difficile risalire a colui cui e' stato ricaricato

per sbaglio); per questo apro una parentesi:

PROPRIO PER QUESTO MOTIVO, RITENGO CHE SE IO RICARICO IL TELEFONO A GIACOMINO

FACENDOGLI PAGARE UN PO' DI MENO, E LA TIM GLI ROMPE I COGLIONI

(COSA DIFFICILE TRANNE SE SI ACCORGE CHE E' STATO FATTO ILLEGALMENTE) LUI

PUO' BENISSIMO DIRE: "CHE CAZZO VOLETE DA ME, NON MI ROMPETE I COGLIONI,

AVRETE FATTO UNO SBAGLIO VOI O QUALCHE DEFICIENTE HA RICARICATO IL MIO

TELEFONINO AL POSTO DEL SUO, ANDATE A CAGARE BASTARDI RINCOGLIONITI !!!"

O magari anche con parole piu' delicate, comunque ho reso l'idea.

Ora vi allego qui sotto le considerazioni di un amico che ha provato via

centralina meccanica una "penetratio" del green, troverete anche alcuni

miei commenti con c:\cavallo> prima :-)

==========

THE PERFECT PHREAKER

---

step one: trying to access on a telecom server, chapter 1

ovvero come farsi beccare e finire in galera..... (speriamo di no)

In data XXXXX tentavo di collegarmi al numero ricevuto dal cielo e constatavo

con (non ti dico quanta) sorpresa che il terminale, una volta in carrier

detect, non fa semplicemente un cazzo.

Se ne sta zitto, non ti dice niente, non comunica nulla e sulla linea c'e' SOLO

ED ESCLUSIVAMENTE la portante (la portante e' quella forma d'onda che viene

modulata sulla linea e che serve per "portare" (cazzo, strano!) i segnali veri

e propri e che mantiene il collegamento anche senza l'invio di dati.)

Praticamente e' in modo originate e non in answer, almeno suppongo.

E' come se ti stesse chiamando lui.

Procedendo ai tentativi piu' svariati, ho constatato che:

Il server se ne sta in attesa, aspettando "qualcosa", magari il seriale

tanto nominato, oppure aspetta di sapere che tipo di terminale si sta

collegando (magari e' usato anche da altre aziende per altre cose, non so)

con i soliti enter doppio space, ed esc, ti sconnette.

Solo enter o solo esc ti sconnette.

Pero' ti fa scrivere quello che vuoi, chiaramente non restituisce l'echo

dei caratteri, e quando dai l'invio ti sconnette probabilente per la pass

sbagliata od il seriale scazzato.

Riassumendo:

IL TERMINALE, PUR NON COMUNICANDOTELO, VUOLE UNA PASSWORD O UNO USERID OPPURE

NECESSITA DI SAPERE CHI E' DALLA'ALTRA PARTE.

Per la serie "gli esempi del cazzo" eccoti il paragone:

Immagina di essere un informatore e di dover comunicare informazioni riservate ad un altro tizio del cazzo.

Sicuramente non andrai in giro a dire "Oh, io devo dire un'informazione riservata!, c'e' mica il tizio che cerco?? ehi?? mi sentite??"

Te ne staresti zitto, e aspetteresti che il tizio ti venga a dire "SONO IO, DIMMI TUTTO".

Questo e' quello che fa il server laggiu' alla telecom.

Ma come stracazzo fare per sapere COSA vuole, quante pass, quanti id, 1 alla volta? 2 alla volta? boh? un brute force potrebbe essere l'unica cosa, ma su quali basi compilare la sorgente per le pw?

In che ordine fornirle?

Non credo che siano solo robe come admin, root, sysop, etc.., ma robe come 9255ui5gilojh5giu5gpi32u5gk32jhvrljehfbvd9pc7t\

(per il seriale della postazione, si intende).

Con un server che ti prende per il culo e ti riattacca in faccia appena scazzi, e' un'impresa.

Mi sa che si ritorna al seriale della "postazione", l'unica cosa che forse, neanche i dealers possono (anche volendo) vedere!!!!!!!!!!!!

CREDO CHE LO POSSA CONFIGURARE SOLO L'ASSISTENZA

Infatti ieri stavo pensando che la telecom non puo' essere cosi' stupida da non considerare che su 300 (ipotizziamo) centri di ricariche in italia, almeno 1 abbia un'operatore che ne puo' capire qualcosina di hacking e phreaking..

Allora, diciamo che si siano prevenuti, e si siano attrezzati:

Io avrei scelto i modi piu' sicuri per farlo:

1- Farsi un software fuori standard.

2- Utilizzare per l'invio e la ricezione due protocolli diversi: ppp / ftp .

Gestire l'invio dei dati in maniera complessa: (l'ftp di cui parlavi, credo

serva proprio per questo) loro si collegano, il software inizia la

negoziazione, senza il sw la connessione non prosegue nemmeno.

Una volta connessi il server resta in attesa dei dati che vengono poi spediti

in FTP! Poi aperti, elaborati etc.. e roba varia..

Quindi bisogna pensare ad una vera e propria DOPPIA connessione

PPP-TCP/IP,FTP!

E a questo punto, io direi MEEEERDDDDA.

3- E NON MENO IMPORTANTE, LA STORIA DI "VERIFICA DEI DATI DELLA POSTAZIONE

IN CORSO" MI FA VENIRE IN MENTE QUALCOSINA... HAI PRESENTE UN BEL TRACE

FATTO PERBENINO CHE SE IL NUMERO TELEFONICO NON E' QUELLO DEL CENTRO TIM

"DA GINO" NON TI ABILITA??

c:\cavallo> Secondo me questa e' 'na cosa un po' esagerata, non arriviamo a

livelli X-Files, forse puo' essere pero' una cosa simile ai servizi fax on

demand, il centro TIM inserita la password viene poi automaticamente

richiamato dal server che stabilisce la comunicazione.

P.S.:

LE INFO NON VENGONO INVIATE IN TEMPO REALE PERCHE' QUANDO HANNO FINITO DI

INSERIRE I DATI, TI CHIEDONO "TUTTO A POSTO, VADO?" E PREMONO IL

PULSANTE PER INVIARE...

c:\cavallo> Questa e' una cazzata, i dati vengono si' inviati in tempo reale

anche perche' x esempio quando metti il codice fiscale il terminale si mette

a lavorare e dopo un po' ti restituisce i dati della persona (se presente)

presi dal database di Sorella TIM.

Non ho mai visto un server ftp che richiede 2 pw. quando hai l'accesso

root, o ce l'hai o non ce l'hai E SERVE UNA SOLA PW.

c:\cavallo> Fino a qui ci arrivo anche io, ma chi ci dice che e' un vero

ftp? potrebbe, anzi sicuramente e', essere un sw dedicato!!

Quindi e' ipotizzabile:

una connessione tcp/ip "rigirata" (difficile connettersi, perche' tutti pensano

che il server non risponda e invece devi essere tu a farlo, sono configurazioni

che pochi si ricordano, ormai lo standard le ha cancellate..), cioe' tu in modo

answer e lui in originate (sono delle configurazioni dei modem), con una

autenticazione di sw, numero tel. (cazzo!) e poi di user.

Il server poi potrebbe comunicare al software (eventualmente) l'algoritmo "del

giorno" (piu' sicuro cambiarlo una volta al giorno) per quanto riguarda

l'impacchettamento dei dati rigurardanti l'utente.

Poi, effettuato l'inserimento, il sw fa un calcolino secondo il suddetto

algoritmo, richiede di poter inviare, il terminale "devia" in ftp e invia il

tutto al server (mooolto complesso).

Il server lo apre, (tipo un mailer door) lo elabora e ti accredita il tutto.

Questa elaborazione, etc.. spiega il leggero ritardo di accredito.

==========

E' Tutto, carissimi compari, fate buon uso di queste infos.

L'uomo chiamato Cavallo

P.S.: Evitate di Postare questo articolo sui NewsGroup.

Cavallo De Cavallis [S0ftPj98]

4.5 Trucchettini e curiosità varie

In questa sezione raccogliamo tutti i trucchettini che sono sul nostro sito, poca cosa ma è quello che abbiamo.

4.5.1 Trasformare un Etacs in uno scanner

E' una cosa semplicissima intercettare chiamate di etacs dato il fatto che i segnali radio dell'etacs non hanno alcun tipo di decodifica. Il miglior modo per farlo è usare uno scanner ma anche un telefonino va piu' che bene. Ogni telefonino infatti è un potenziale scanner visto che ha al suo interno una ricetrasmittente sui 900

Mhz. Ora basta bypassare le funzioni standards del telefono per utilizzare questa ricetrasmittente come ci pare. Io , avendo il motorola , so come fare solo su questo telefonino ma sicuramente anche con altri è possibile fare cose del genere. Ecco le istruzioni da seguire se avete un motorola etacs

Aprire la batteria e verificare che ci siano tre contatti sul telefono e che il contatto centrale sia leggermente un po' piu' abbassato degli altri due esterni.

Verificato cio' mettete un pezzettino di stagnola sul contatto centrale e quindi reinserite la batteria.

Riaccendete il telefono e no panik! Il vostro teleofnino comincera' a scrivere strani numeri sul display , ora è entrato in Test-mode! Premete cancelletto e vedrete la scritta Tac5 sul display. Poi scrivete 08 e quindi di nuovo cancelletto.

Il vostro telefonino si è trasformato quindi in uno scanner! Scrivete un canale radio compreso entro 1101 e 1199 e premete cancelletto una volta finito di scrivere il canale e potrete sentire tutte le telefonate che vengono fatte nella cella in cui vi trovate! ES: per ascoltare le chiamate che vengono fatta nel canale 1120

dovrete digitare 1120#.

4.5.2 Le ultime 1000 lire

di Chatrobot

Se siete rimasti con sole mille lire nella scheda del vostro ricaricabile fate l'ultiuma telefonata e potrete parlare anche per cinquanta ore!!

4.5.3 Segreterie comunque

di Chatrobot

La tua fidanzata lascia il telefonino staccato senza segreteria telefonica e tu stai provando da 3 ore a chiamarla senza successo? O vuoi semplicemente riempire la segreteria telefonica del cellulare di un tuo conoscente con spernacchiate varie, ma non ha la segreteria abilitata?

Ebbene, puoi mandare messaggi alle segreterie telefoniche degli utenti GSM - anche se non hanno abilitato il servizio -.

Come? Il principio e' in realta' semplicissimo.

L'abilitazione della segreteria telefonica cellulare in realta' non e' altro che una deviazione delle chiamate in arrivo verso un secondo numero, molto simile al proprio numero di telefono.

Chiamata ---> Numero 1 ---> Numero 2

(Cellulare) (Segreteria)

Dunque, se con un altro cellulare GSM chiamiamo DIRETTAMENTE il secondo numero, quello della

segreteria, potremo accedere al servizio, anche se l'utente non ha attivato la deviazione chiamate verso quell'altro numero! Quando l'utente accendera' il cellulare, ricevera' un messaggio SMS che lo avvertira'

della presenza di un certo numero di messaggi nella segreteria.

Ecco a quali numeri telefonare:

Per i cellulari TIM:

Prefisso / 55 / Numero

Per i cellulari OMNITEL:

Prefisso / 20 / Numero

4.5.4 Trucchi col trasferimento Omnitel

di Telecomico

con le carte ricaricarbili omnitel chi setta il trasferimento di chiamata non lo paga.

Quindi si puo' utilizzare accoppiato ad un abbonamento con you & me rifemento quella ricaricabile (non so se e' ancora possibile fare you & me con ricaricabili), puoi chiamare chiunque a tariffa bassa!

fino a mesi fa si'.. non io personalemnte... comunque il trasferimento gratuito l'ho verificato di persona...

alcuni dicono che se ne abusi allora te lo fanno pagare... boh...

4.5.5 Rendere ricaricabili i Nec p7 a sbafo!

di Space Navigator

Un modo per rendere i Nec p7 ricaricabili senza pagare i centri di assistenza (lo so, non c'entra niente con la Telecom, ma almeno puo' essere considerato un po' phreaking....):Accendi il telefono e digiti ...

*26041969# F MR 76 MR # 01 MR # 71

adesso sei entrato nel NAM-1 ovvero nella programmazione della linea N.1, (il NEC supporta 4 linee telefoniche sullo stesso telefono, Tim ovviamente no).Puoi scorrere i vari settaggi premendo il tasto #.

Quando arrivi alla voce EMERGENZA *** al posto dei tre * inserisci il munero 314 e continui con #, ti si attiva una voce supplementare Cambio-PIN, la setti a SI e completi il giro con #.

Per memorizzare il tutto esci con C prolungato che ti riporta in TEST-MODE e esci con MR # 02.

Adesso battendo F6 + il tuo numero di blocco ti si e' attivato il sottomenu 6xxxx8 dove chi autentica il telefono inserira' il numerone a16 cifre.

ATTENZIONE: TUTTI i NEC P7 hanno questa procedura, ANCHE QUELLI CHE NON E' POSSIBILE

CONVERTIRE A RICARICABILI per un bug software.

4.5.6 Bug Ericsson 688

di Scanman

questo dovrebbe essere un trucco per chiamare gratis (se il network gsm lo consente - credo che sia un bug)

Chiama un numero, aspetta finchè "connecting" appare scritto sul display poi premi:

CLR, 0, #,

(a questo punto appare la parola 'auto sul display)

poi NO e poi di nuovo NO (per spegnere il telefonino)

E vedrai che così il telefono sarà spento ma la luce verde sarà ancora accesa e che potrai parlare nonostante il telefono sia spento.

Per spegnere il telefono dovrai togliere la batteria.

4.5.7 Bug del Motorola 7500

Prendete un telefono cellulare MOTOROLA 7500 e alzate il volume dello squillo e della ricezione al max, poi tramite le funzioni del menu' disattivate lo squillo del telefono.....a questo punto con un

normale telefono di casa o un telefono di una cabina chiamate il numero del MOTOROLA 7500 (mi

raccomando non rispondete con il MOTOROLA !!! fatelo squillare liberamente !!) mentre il telefono con cui stiamo chiamando il cellulare emette il segnale di libero, provate a parlare normalmente....sul motorola (che indica sul display lo squillo....mi raccomando non aprite lo sportellino) si sente pari pari la voce della persona all'altro capo !!! Naturalmente nessun addebito in merito...visto che il telefonino non viene aperto....quindi e'

possibile parlare in una direzione in modo gratuito... Questo trucco funziona su tutti i motorola 7500 che io ho provato.....e su alcuni 7200, sul 8700 no.....

4.5.8 Cellulari in TV

di Ulixes

Allora, da qualche parte dovrò pur cominciare.....

Ho trovato un interessante falla per ascoltare su normali vecchi televisori manuali le chiamate dei telefoni cellulari. I canali TV UHF 70-83 sono quelli su cui bisognerà sintonizzare il TV per poter origliare.

La sensività non è delle migliori, tranne se non si è in città o in luoghi sensibili a quelle comunicazioni.

PS non se se ciò che è stato descritto è illegale o meno, ma vi assicuro che funziona alla meraviglia.

4.5.9 SMS Gratis

di Pietro

Provate ad impostare come SMSC +4792001000 (Netcom) ed ad inviare un SMS verso un utente

TIM.Risultato: su alcuni numeri (il mio per esempio, ho la Tim Card!) dopo circa 30 secondi viene fuori

"Messaggio non inviato" ... ma il messaggio ha già raggiunto il destinatario ed io non ho pagato una lira!N.B: Da TIM CARD mia a numeri TIM = OK, da mio Libero a numeri TIM = OK ma non da quello della mia

ragazza, lì dice subito "Messaggio non inviato" e non arriva nulla.Fate qualche prova e fatemi sapere.

4.5.10 SMS e bug OPI

di Blum

SMS

Sembra che usando il +491722270300 per spedire SMS non si spenda niente, però non ne sono assolutamente certo. Inoltre sembra che con alcune schede funzioni tipo la Personal 195 e con altre no tipo la Personal City

BUG OPI

Se si ha una una scheda prepagata OPI e si arriva a 0 lire di credito sembra che ti permetta comunque di spedire SMS chiaramente a sbaffo (credo comunque un massimo di 10 dopo di che tenta di fare l'addebito e dovrebbe disabilitare la scheda)

4.5.11 Chiamare gratis con gli Ericsson

di CDP

Utilizzando una scheda prepagata GSM OMNITEL (con TIM gli scatti vengono conteggiati... occhio!) ed un telefono Ericsson è possibile, a quanto pare, chiamare a scrocco, almeno fino a quando non vi bloccheranno la SIM (ragionevolmente dopo una settimana di uso intenso del trucco, anche se conosco gente che ha scroccato per anche 2 settimane).

Ericsson GH688

Chiama un numero, aspetta finchè "connecting" appare scritto sul display poi premi:

CLR,

0,

#, (a questo punto appare la parola 'auto sul display)

poi NO e poi di nuovo NO (per spegnere il telefonino)

E vedrai che così il telefono sarà spento ma la luce verde sarà ancora accesa e che potrai parlare nonostante il telefono sia spento.

Per spegnere il telefono dovrai togliere la batteria.

Sui nuovi modelli bisogna tenere premuto NO senza lasciarlo (la seconda volta) altrimenti il cello si spegne.

Ericsson Gf788e

Comporre il numero poi subito:

CLR,

NO

e poi NO tenendolo premuto.

Per il GF 788 dovrebbe funzionare quello del Gh688.

Ericsson GA628

Comporre il numero e poi:

CLR,

NO fino a spegnere il telefono.

Nei vecchi telefoni il NO può essere rilasciato mentre per i nuovi bisogna tenerlo premuto.

4.5.12 5110/6110 Spione

di Blum

Cortocircuita i pin 3 e 4 di un Nokia 5110 o 6110, ti apparirà la scritta "con auricolare".

Imposta la suoneria a NO e risposta automatica a SI.

Hai cosi' ottenuto un apparecchio che, in automatico e silenziosamente, risponderà alle tue chiamate, a ti invierà quello che "sente" nell'ambiente.....

Disegno dei pin di un 5110

tastiera

_____

| |

| 1 O 2 |

| x3456789x |

|_____|

batteria

4.5.13 Possibile bug 8700

di Blum

Tramite un procedura semplice si può conoscere il codice blocco del telefono.

Quando appare la scritta Cod Blocco basta premere Menu, andare in cambio

codice blocco e digitare 0000.

Ecco tutto.

4.6 Codici segreti di cellulari GSM

Questa sezione raccoglie tutti i codici segreti per intervenire sulle impostazioni avanzate dei cellulari GSM

divisi per casa di produzione. Tutti i codici sono stati estratti da Mobileworld e da altri siti, e tradotti da CDP.

4.6.1 Alcatel

Alcatel One Touch Easy

Scrivere 000000 e premere *

Appare: Secret Menu

TRACES Menù idicatori canale

ARRETS - ?

VIDER ARRETS Premere OK e il telefono risponde: This action is executed!

CTRL CHARGE Mostra il voltaggio del caricabatterie e della batteria.

DAMIER Mostra test

Il Master Code per il "MENU code" e il "Prod. code" dell' Alcatel One Touch Easy è 25228353.

So che V13 e V14 vengono mostrati alla fine di *#06#. Nellla versione V13, una novità è che viene mostrata una "-" alla fine della linea del display per le parole lunghe.

Alcatel Mobile Phones

Molti di questi telefoni hanno l'SP lock, possono cioè essere usati solo con certi fornitori di servizio. Questa funzione può essere disattivata solo chiedendo il codice speciale all'Alcatel stessa o al fornitore del servizio (TIM o OMNITEL in Italia). Si dice che esiste un programma che permette di risalire a questo codice a partire dall'IMEI. Questa notizia non è verificata.

IMEI 3300 1453 1139 420

Se attivato con una scheda TELSTRA, il telefono si avvia con un:

"PRODUCT CODE"

"VAL. => OK"

Quindi si inserisce 025121992 OK

"ENTER SPECIAL CODE"

**05* come i Motorola

"UNBLOCKING"

" PUK ? "

10608CC2*. Anche questi due da Vodaphone funzionano 906081C2* 15900807*

"UNBLOCKING"

" PIN ? "

0000*

"UNBLOCKING"

"PIN AGAIN "

0000#

Sembra che debba trovare il PIN Perchè a questo punto il telefono si riavvia

Software releases

HC400 sul retro ha uno sticker con su l'IMEI e la versione software. L'Alcatel ha così diviso l versioni software:

1.x senza Cellbroadcast

5.x con Cell broadcast

la più recente software release dell' HC 1000 è la AK1 03

Alcatel HC600/800/1000

*#06# IMEI e Software Version (escluso HC600).

Questi sono i pinout dell' HC600 gli stessi dell' 800/1000 credo.

1 3 5 7 9 11 13 15

I I I I I I I I

O

O 17

I I I I I I I I

2 4 6 8 10 12 14 16

1 Vbat_ext

9 SDA_E

2 EMMI_PAE

10 GND

3 Mic

11 GND

4 EMMI_OPE

12 DC_IN (charge)

5 GND

13 Speaker

6 EXT_EMET

14 MARCHE

7 SCL_E

15 DC_IN (charge)

8 EXT_RECDIT

16 GND

17 Antenna+internal switch (int/ext)

4.6.2 Ericsson

ERICSSON 198

Per vedere l' IMEI: *#06#

Per resettare i timer 904060 <FUNCTION> <FUNCTION> SEND

Per ativare le modalità di Programmazione 923885 <FUNCTION> <FUNCTION>.

Potreste dover inserire questi codici con il tasto funzione premuto.

ERICSSON 218/337

Per vedere l' IMEI: *#06#

Per vedere la versione del Software: -> * <- <- * <- * CLR (Fare attenzione)

Per attivare l'SP lock <- * * <- (Permette di usare la SIM sono con un gestore di telefonia) Premere Yes per bloccare e No per sbloccare. Per disattivare questa funzione potete anche usare i codici qui sotto. USATE A VOSTRO RISCHIO E PERICOLO

Almeno sul 337 c'è un sottomenù: Enter SPCK-code. Ci sono 5 possibilità, e vengono mostrate (05

attempts). All'ultima possibilità il telefon suona per avvertirvi, 'this is the final try', quando entrate nel menu'...

Un codice errato fa uscire dal menù, così da non farvi restare bloccati... quando sbagliate il codice per 5

volte il menù viene disattivato, e verrà mostrata la scrittat: 'Not allowed' quando si digita <-**<-

Un "secret test mode" può essere raggiundo con un GH337. Dovrebbero esserci due modi:

> * < < * > * software version, come 940810 1310

> * < < * < * software version, come 951024 1054

Dopo aver avuto accesso a questo menu, i tasti < e > scorrono il menù. Sembra che ci siano diversi menù a seconda della versione del software.

I numeri delle versioni del software sembrano essere apparentemente una data e orari.

la versione 940810 1310 ha:

TEXT CHECK - mostra 254 messaggi

INIT EEPROM MMI - resetta i settaggi NVRAM (User Settings).

Altri, probabilmente della versione più recente:

FLASH - riavvia il telefono al punto dell'inserimento del codice PIN.Non si può 'Killare' un 337

premendo YES quando chiede "FLASH?", devi prima collegarlo a 5/12 volts per poter cancellare la memoria flash.

1-ROW TEXTS - scorre 174 messaggi di una linea con i tasti <>

n-ROW-TEXTS - scorre i messaggi a tutto schermo con < e >

la versione 950626 1405 ha:

CXC (number) - Application software's "product number". Il GH337/GF337 è sempre "CXC 125 005"

PRG - Indicazioni per programmare.

Programmare il 337

Setttare ComPort a 9600bps, 8 data, 1 stop, no parity.

Accendere il telefono con "NO/ENDpwr".

Durante la seguenza di avvio il telefono invierà ">>"

(ASCII 62 decimal). Entro un secondo, inviare questa sequenza "TP1<CR>".

(Abbiamo usato il programma PROCOMM PLUS con questo script "eric.asp")

[proc main]

[start:]

[

]

[waitfor ">>"]

[pause 1]

[transmit "TP1^M"]

Se tutto è andato bene dovresti ottenere "OK".

Provate TEST PROGRAM inviando i comandi seguiti da <CR>:

PROG 0 (Test Program product number info)

PROG 1 (Test Program product date info)

PROG 3 (Main Application product number info)

PROG D (Main Application product date info)

Programmare la Calcolatrice e il Channel Indicator/RBS

Per abilitare, inviare:

EEWR 047A 01

Aspettare l'OK, Spegnere* e staccare i cavi. Accendere e scorrere i menù.

Per disabilitare:

EEWR 047A 00

Resettare il blocco elettronico

Per resettare il blocco dovrete cancellare l' EEPROM nel range 045B - 0466 inviando questi comandi:
EEWR 045B 00

EEWR 045C 00

EEWR 045D 00

EEWR 045E 00

EEWR 045F 00

EEWR 0460 00

EEWR 0461 00

EEWR 0462 00

EEWR 0463 00

EEWR 0464 00

EEWR 0465 00

EEWR 0466 00

Disabilitare il Service Provider Lock

Per disabilitare inviare:

EEWR 1587 00

Per abilitare:

EEWR 1587 01

Comandi sperimentali - Usate a vostro rischio

Per prendere i settaggi del software:

PREA <bank> <address> <bytestoread>

Bank range : 00..7F

Address :

0000..BFFF

Bytestoread : 0000..BFFF

I valori in più alla fine sono i checksum per i byte di memoria rstituiti. Il formato sarà sempre 0000 e non 00.

PREA FF

application checksum, impiega qualche secondo.

Note sul PH 337

1. La calcolatrice non è disponibile su tutte le versioni di Software.

2. Calc/RBS mode non disponibile sui GH337 nelle versioni software precedenti la R2A

3. i tentativi SPCK possono essere cambiati da 5 a 50

4. L'istruzione LIME fa apparire ERR ma non danneggia il telefono.

5. L'istruzione IMEI restituisce il numero IMEI.

6. Rispondendo con YES a FLASH? Distrugge l'unità.

COSE DA PROVARE

Settare ComPort a 115200bps, 8 data, 1 stop, no parity e vedrete tutti i comandi sullo schermo. Fate una chiamata e vedete cosa accade...

ERICSSON 318/388

IMEI: *#06#

Software Version: -> * <- <- * <- * CLR (Fare attenzione)

L'Ultima versione del software è sotto Phone Info.

Per regolare bene il suono e eliminare gli eco, mettete il 388 in un kit viva voce HF 2600.

Chiudete tutte i finestrini, spegnete il motore e digitate * # * # 3. Il telefono si regolerà automaticamente in pochi secondi.

SP lock <- * * <-

Yes per bloccare e No per non bloccare.

Programmare la flash di un 388:

1. Connettere il 388 al cavo con un RS232/TTL.

2. Settare Comport a 9600bps, 8 data, 1 stop, no parity.

3. Power ON, attendere "2" e inviare "OB" al telefono. Non premere ENTER.

4. R dovrebbe apparire sullo schermo.

5. inviare pre_xxx.bin al MS.

6. dovrsti ricevere ">".

7. inviare "0B" di nuovo.

8. R dovrebbe apparire sullo schermo

9. inviare prodload.bin al MS.

10. riceverete ">".

Al momento non ho i files .bin. Provate su MobileWorld.

Programmare il Channel Indicator o RBS

Per abilitare inviare:

EEWR 3EE 1

Attendete OK , spegnete* il telefono e scollegate i cavi. Accendete il telefono e scorrete tra i menu.

per disttivareinviare:

EEWR 3EE 0

Resettare il blocco elettronico

Per resettare il blocco dovrete cancellare l' EEPROM nel range 03CF to 03DA inviando questi comandi:
EEWR 3CF 00

EEWR 3D0 00

EEWR 3D1 00

EEWR 3D2 00

EEWR 3D3 00

EEWR 3D4 00

EEWR 3D5 00

EEWR 3D6 00

EEWR 3D7 00

EEWR 3D8 00

EEWR 3D9 00

EEWR 3DA 00

COSE DA PROVARE

Settare ComPort a 115200bps, 8 data, 1 stop, no parity e vedrete tutti i comandi sullo schermo. Fate una chiamata e vedete cosa accade...

SPEGNERE

Dovreste premere no uun po' di volte finchè il prompt Shut down? appare, premere YES e il telefono si spegnerà.

Leggere le Channel Info

|-------|-------|-------| D

| | | | I

| 1 | 2 | 3 | S

|-------|-------|-------| P

| | | | L

| 4 | 5 | 6 | A

|-------|-------|-------| Y

1. 3 info diverse a seconad dello stato del telefono.

o a. Il telefono non fa nulla: "Bxxx". "B" è "Broadcast channel" (a logic GSM channel) o b. Chiamata in corso: "Sxxx". S è "Stand Alone Dedicated Control Channel" SDCCH.

o c. Chiamando: "Txxx". "T" è Traffic channel. Le "xxx" indicano il numero del canale, 1-124.

2. Rx Level.I valori vanno da 0 a 63. Rx Level indica l'intensità della ricezione. 0 indica un segnale di -

110dBm. 63 è circa -45 -50dBm.RXLEV è misurato in dBm in modo che il segnale in ingresso equivale a -

110.5+RXLEV così che un RXLEV a 50 equivale a un'intensità del segnale di ingresso di -50.5 dBm (con un errore di 0.5dBm)

3. Output power in dBm.

4. Timeslot usato al momento. Si vede quando si fa una chiamata.

5. Rx Quality. Rx Quality indica quanta correzione di errore è necessaria per parlare. 0 indica nessuna, e come aumenta udrai più PING e PONG. Se RxQ è maggiore di 5, hai ottime probabilità di perdere la chiamata. RxQuality va da 0 a 7.RXQUAL viene misurata con una tavola in modo che la biterrorrate o BER

siainteressante e misurata in %

RXQUAL table

0

BER < 0,2 (%)

1

0,2 < BER < 0,4

2

0,4 < BER < 0,8

3

0,8 < BER < 1,6

4

1,6 < BER < 3,2

5

3,2 < BER < 6,4

6

6,4 < BER < 12,8

7

12,8 < BER

6. Timing advance. TA viene misurato in halfbits cosicchè la distanza dal BTS può essere così calcolata

=1,11*TA/2. I valori del TA vanno da 0 a 63. Questo indica anche quanto siete distanti dalla base in blocchi di 550 metri, fino ad un massimo teorico di 35.2km.

ERICSSON 788

IMEI *#06#

Software Version * -> * <- <- * <- *

Service Provider Lock * <- <- * ma viene chiamato ME lock. Dopo averlo selezionato ci sono due opzioni su un altro menù(Lock to Network e lock to Network subsect).

Codici per Ericsson GH688 GH388 GH628 **GF788 GF768**

*#06# IMEI (International Mobile Equipment Identity)

*#0000# Resetta la lingua in Inglese.

>*<<*<* firmware revision information (software release)

CXC125065 - internal product code.

PRG - Firmware revision (date & time stamp).

970715 1515

>*<<*<*> 1-row text strings. Mostra tutti i txt di una riga. (298)

>*<<*<*>> n-row text strings. Mostra tutti i txt di più righe. (160?)

ERICSSON Pin-Outs 2xx & 3xx Series

1

In Voice

2

In +5V=External Power, 0V=Battery

3

Out Ext Speak control

4

Analog GND

5

Out Voice

6

Out +5V=POWER ON, 0V=POWER OFF

7

Out Charger control

8

Digital/DC GND

9

In 0V=normal,+5V=test, +12V=test+flash

10

In Hook

11

In TTL serial in

12

Out TTL serial out

13

In 0V for aprox 1 sec = POWER ON/OFF

In DC Power supply

ERICSSON GH688 Pin-Outs

1 = + external power supply

2 = RS232 input (TTL)

3 = GND (digital)

4 = RS232 output (TTL)

5 = +5V output

6 = Test

7 = Mute

8 = Internal/external

9 = GND (analogic)

10 = ?

11 = BF in

12 = BF out

1: Per caricare la batteria e alimentazione esterna.

Non fa funzionare il telefono senza la batteria

Voltaggio: 7.2V con almeno 600mA.

2: RS232 serial line input a livello TTL (0/5V).

Quando il telefono è acceso, questo PIN è a "0" (?!?!?), contro ogni logica.

Connettetevi la RS232/TTL anche se l'output è 1!!!

3: GND digital....no comment!

4: RS232 serial out put a livello TTL (0/5V). Quando il telefono è acceso è a 1.

5: +5V output con telefono acceso.

6: Mode test. Generalmente è a 0. Per andar ein Test mode, spegnere il telefono, mettere il Pin a 1 (+5V), accendere il telefono. In questo modo la seriale lavora a 115200 invece che ai soliti 9600.

7: Mute. Di solito a 0, Va a 1 Quando si scorre o durante la conversazione.

8: Se aperto, Il microfono e lo speaker interni sono accesi. Se a 0 sono abilitati quelli esterni.

9: GND analogic (no comment).

10: Mistero. Quando è a zero sembra che speaker e microfono si attenuino.

11: BF in (no comment...)

12: BF out (no comment...)

3. Motorola

MOTOROLA 6200/7500/8200/8400/8700

Attivare l'RBS (Engineering Menus):

[pause] [pause] [pause] 1 1 3 [pause] 1 [pause] [ok]

(pause indica il tasto * tenuto premuto)

Premere ora [MENU] scorrere fino a 'Eng Field Options' con le frecce e attivarlo.

Disattivare l'RBS (Engineering Menus):

[pause] [pause] [pause] 1 1 3 [pause] 0 [pause] [ok]

Funziona sui 6200,8200,1-888,7500,8400 e gli StarTac GSM con una versione del

software successiva alla .27.

Opzioni dell'Eng Field Options

Eng Field Options

Active Cell

RxLev -55 Potenza ricevuta in dBm

NCC 0

National Colour Code, usato per

identificare il colore

BCC 7

Broadcast Colour Code, anche questo serve

a scopi identificativi

MSTxPwr 35 Massimo potere di trasmissione possibile 35dBm

circa 3.2W

C1 003

Indica la qualità di controllo del segnale

inviata costantemente

dall'RBS.

Se il segnale rimane

negativo per 5 secondi,

il telefono cambia cella.

Time Adv xxx xxx è un numero. Moltiplicato per 550da' la

distanza

in metri dall'RBS RBS (Radio Base

Station), in meters.

Adjacent Cells

Adj Cell 1

Channel 0033

Numero del canale

RxLev -65

Potenza del segnale ricevuto in dBm

BCCH Decode Dovrebbe significare che è capace di decodificare

la channel

information contenuta nel BHCC

RxLevAM -104 Ricezione Minima consentita, comparata con RxLev

-65 si

si ottiene C1 (che è 39) e viene reinviata

alla base come

indicatore della forza del campo

MTxPwr 35 Aain max consentito

C1 003

??

NCC 0

National Colour Code

BCC 6

Broadcast Colour Code

System Parameters

Combined Off

??

AcsClas 0000

Consente diverse priorità -(questo gestore

non lo supporta).

MCC 505

Mobile Country Code, 505 per l'Australia,

240 per la Svezia etc

MNC 01

Mobile Network Code, 01 02.. a seconda del

gestore

LAC 08720

Location Area Code, dove siete.

CellID 00473 Base Station Identity

T3212 005

Tempo tra gli aggiornamenti periodici

della rete

(o ore o minuti che mancano. non sono

sicuro)

BS-PA-MFRM 4 ??

XZQTY 14.3 ??

Motorola Flip Pinout:

ANT- (O) | | | | | | | | | |

10 9 8 7 6 5 4 3 2 1

parte superiore (Schermo)

1) Audio Ground

2) Ext b+

3) T Data

4) C Data

5) R Data

6) Logic Ground

7) Audio Out - on/off

8) Audio In

9) Manual Test

10) Battery Feedback

4. NEC

NEC G8/NEC G9/NEC Kiss/NEC Sportz Digital

IMEI: *#06#

5. **Nokia**

NOKIA 1610

IMEI *#06#

Software Version *#170602112302#

L'ultima versione è sotto Phone Info

Pinouts

1

GND

Digital Ground

2

V_OUT Output per accessori. (Min/Typ/Max - 3.25V...10V

- Output Current 50mA)

3

XMIC

Input dek microfono esterno e identificazione accessori

*TYP/MAX: 8...50 mV(Il valore massimo corrisponde a

0dBm Network

LIVELLO CON GUADAGNO AMPLIFICATORE IN

INGRESSO SETTATO A 20 dB ,Il valore tipico

è il massimo -16 dB)

ID

Accessory Identification

*1,7...2,05 V HEADSET ADAPTOR connesso

*1,15...1,4 V COMPACT HANDSFREE UNIT connesso

4

NC

Non Connesso

5

NC

Non Connesso

6

MBUS

Serial Control Bus

*Logic Low Level: 0....0.5V

*Logic High Level:2.4V....3.2V

7

NC

Non Connesso

8

SGND

Signal Ground

9

XEAR

Speaker esterno e controllo Mute

*Min/Typ/Max: 0....32....500 mV (il livello tipico

corrisponde a -16 dBM)

Network Level col volume settato a un valore nominale

di8dB sotto il massimo

Maximum 0 dBM m,assimo guadagno volume codec -6dB)

Mute ON (HF SPEAKER MUTE):0...0,5 V d.c.

Mute OFF (HF SPEAKER ACTIVE): 1,0...1,7 V d.c.

10

Hook

Hook Signal

*Hook Off (Handset in uso): 0....0.5V

*Hook On (Handset in Uso): 2.4V....3.2V

11

NC

Non Connesso

12

V_IN

Voltaggio del caricabatterie (Max 16V)

NOKIA 2010

IMEI *#06#

Software Version *#9999#

NOKIA 2110 / PHILIPS 747

IMEI *#06#

Software Version *#9999#

L'ultima versione è sotto Phone Info

Il tipo è NHE-1XN

Per bypassare il SIM Lock sul 2110;

Accendere il telefono, Quando chiede il codice di sicurezza,

premere 112 e dopo il pulsante di invio.

ora premere velocemente # e invio, end, invio e invio.

Questo disattiva il Sim Lock fino alla prossima volta in cui spegnerete il telefono.

NOKIA 2110e/i / PHILIPS 747II

IMEI *#06#

Software Version *#170602112302#

Con l'ultima versione del software digitare invece *#682371158412125#

L'ultima versione è sotto Phone Info

Settimana e anno di fabbricazione: *#3283#

Sui telefoni fabbricati prima del 01/01/96 1295 significa December 95, sui telefoni successivi allo 01/01/96

2196 significa la 21esima settimana del 1996.

Per togliere il CAPS LOCK tenere premuto il pulsante dela lettera desiderata.

NOKIA 2110 PINOUT

Pinouts del X100 system connector

ANT 16 9 Connettore caricabatterie

(O) I-I-I-I-I-I-I-I ( ) (o)

CON 8 1

Il simbolo (O) a sinistra è il connettore dell'antenna per i kit per auto. i simboli numerati 16-9 in cima e 8-1 in basso sono i system connector. La ( )è lo soazio tra il connettore e (o) è l'attacco per il caricabatteria da casa.

PIN

Name

Description

1,9

GND

Terra (Digital)

2

MIC/JCONN

Input audio esterno dagli accessori

o microfono esterno.

3

AGND

Terra analogico per gli accessori

4

TDA

DBUS data trasmesso agli accessori

5

M2BUS

Serial Bidirectional data e controllo

tra telefono e accessori

6

HOOK/RXD2

Hook indication. HP ha un resistore

pull-up di100KE pull-up

7

PHFS/TXD2

Kit mani libere on/off, dati per flashare

le apparecchiature di programmazione.

8,16

VCHAR

Voltagio per la ricarica delle batterie

10

EAR/HFPWR

Audio output per gli accessori e kit mani

libere

11

DSYNC

DBUS data bit sync clock

12

RDA

DBUS dati ricevuti dagli accessori

13

BENA

Power supply all'adattatore

14

VF

Voltaggio di programmazione per la FLASH

15

DCLK

DBUS data clock

DTMF PROGRAMMING

E' possibile programmare un intera sequenza di toni DTMF.

 Digitare il numero.

 Premere tre volte * appare una 'p' (pause).

 digitare la sequenza di toni DTMF , si può usare 'p' di nuovo.

 Memorizzare.

 se selezionate ore questo numero dalla memoria e lo chiamate, il telefono aspetterà qualche secondo (pause) e poi invierà la stringa come DTMF.

 Un'altro modo consiste nel premere * quattro volte: appare una 'w' (wait). Quando la 'w'arriva al punto di essere eseguita nella stringa, 'DTMF' appare sulò menu' del pulsante destro. Quando

premete questo pulsante il telefono inizierà ad inviare i DTMF.

CARKIT PROGRAMMING

Se usate un Kit per auto con un viva voce e un una cornetta addizionale, e volete passare dal vivavoce alla cornetta:

 Premete il bottone del menu a sinistra, e alzate la cornetta.

 Ora siete col vivavoce.

NOKIA 3110

IMEI *#06#

Software Version *#3110#

*#92702689# - il telefono chiederà un codice di garanzia:

Ci sono alcune possibilità qui

6232 (OK) : Mese e anno di fabbricazione

7332 (OK) : Data dell'ultima riparazione

7832 (OK) : Data di acquisto del telefono

9268 (OK) : Serial Number

37832 (OK) : Settare la data di acquisto MMYY

87267 (OK) : Coinferma trasferimento, relativo a quando si aggiorna il firmware.

*#746025625# - il telefono dirà 'SIM CLOCK STOP ALLOWED' o "SIM CLOCK STOP NOT ALLOWED" a seconda della SIM Card.

*#7780# ripristina le impostazioni della fabbrica.

Tipo NHE-8

NOKIA 3810

IMEI *#06#

TSoftware Version *#3810#

NOKIA 5110/6110

IMEI *#06#

Software Version *#0000#

L'ultima versione è sotto Phone Info

Tipo NSE-3NX

*#92702689# Mostra IMEI e numero seriale. Ci sono varie opzioni tra cui scorrere.

- data di fabbricazione (Made: 1197)

- Data di acquisto (Purchasing Date: 1197)

- Data di riparazione (Repaired: 0000)

- Transfer User Data?

Per uscire spegnere il telefono e riaccenderlo.

*3370# attiva Enhanced Full Rate (*efr0#)

#3370# disattiva Enhanced Full Rate (#efr0#)

*4720# attiva Half Rate (*hra0#)

#4720# disattiva Half Rate (#hra0#)

Inserendo questi codici il telefono si riavvierà.

6110 Sim Card Locking

La SIM card può essere bloccata in quattro modi sul 6110.

Country Lock - La lega al paese di appartenenza

Network Lock - La lega al Network

Provider Lock - La lega al gestore di rete

Sim Lock - Lega il telefono a quella SIM

Per vedere lo stato del proprio telefono

#pw+(mastercode)+X#

(mastercode) è un numero di 10 cifre.

X è un numero da 1 a4, indica uno dei 4 precedenti blocchi.

'Sim not restricted' indica che il telefono non è bloccato

Nuove suonerie

Settare SMSC +358405202999 (Smart Messaging)

Inviare un SMS al numero 99999 con la parola TONESnel testo

Appena otterrete una risposta (sarà una lista di nuove suonerie), modificatela in modo che la suoneria che volete ricevere non abbia l'asterisco davanti. Inviate il messaggio al 99999. Il telefono mostrerà NEW

RINGTONE RECEIVED.

NOKIA 8110/8110i

IMEI *#06#

Software Version #8110#

L'ultima versione è sotto Phone Info.

*#92702689# - il telefono chiederà un codice di garanzia:

Ci sono alcune possibilità qui

6232 (OK) : Mese e anno di fabbricazione

7332 (OK) : Data dell'ultima riparazione

7832 (OK) : Data di acquisto del telefono

9268 (OK) : Serial Number

37832 (OK) : Settare la data di acquisto MMYY

87267 (OK) : Coinferma trasferimento, relativo a quando si aggiorna il firmware.

*#746025625# - il telefono dirà 'SIM CLOCK STOP ALLOWED' o "SIM CLOCK STOP NOT ALLOWED" a seconda della SIM Card.

Il tipo di telefono è NHE-6

Pinouts

1

GND

Charger/System Ground

2

V_OUT Output per accessori. (Min/Typ/Max - 3.4V...10V -

Output Current 50mA)

3

XMIC

Input dek microfono esterno e identificazione accessori

*TYP/MAX: 8...50 mV(Il valore massimo corrisponde a

0dBm Network

LIVELLO CON GUADAGNO AMPLIFICATORE IN

INGRESSO SETTATO A 20 dB ,Il valore tipico

è il massimo -16 dB)

ID

Accessory Identification

*1,7...2,05 V HEADSET ADAPTOR connesso

*1,15...1,4 V COMPACT HANDSFREE UNIT connesso

4

EXT_RF Controllo antenna esterna

Min/Max: 0...0.5V RF esterna in uso

Min/Max: 2.4...3.2V uso antenna interna

5

TX

FBUS Transmit

6

MBUS

Serial Control Bus

*Logic Low Level: 0....0.5V

*Logic High Level:2.4V....3.2V

7

NC

Non Connesso

8

SGND

Signal Ground

9

XEAR

Speaker esterno e controllo Mute

*Min/Typ/Max: 0....32....500 mV (il livello tipico

corrisponde a -16 dBM)

Network Level col volume settato a un valore nominale

di8dB sotto il massimo

Maximum 0 dBM m,assimo guadagno volume codec -6dB)

Mute ON (HF SPEAKER MUTE):0...0,5 V d.c.

Mute OFF (HF SPEAKER ACTIVE): 1,0...1,7 V d.c.

10

Hook

Hook Signal

*Hook Off (Handset in uso): 0....0.5V

*Hook On (Handset in Uso): 2.4V....3.2V

11

NC

Non Connesso

12

V_IN

Voltaggio del caricabatterie (Max 16V)

NOKIA 9000/9000i

IMEI *#06#

TSoftware Version *#682371158412125#

L'ultima versione è sotto Phone Info

Anno e mese di fabbricazione *#3283#

Tipo di telefono GE8

NOKIA GENERAL INFO

Queste informazioni sono valide solo per i 2010, 2110, 2110e (e probabilmente gli ETACS 636 e forse 232), non i 1610 o 8110 perche' usano differenti caricatori.

Il caricabatterie della NOkia fornisce 12Vdc limiutati a 770mA. La fine della ricarica viene identificata dallo stesso telefono. Notate che connettendo 12Vdc senza limitare la corrente danneggia sia il telefono che le batterie. A volte il telefono mostrerà la scritta"not charging", Altre volte il transistor all'interno del telefono si brucerà

3. Philips

Philips DIGA

IMEI *#06#

Connect Time *#2558*#

(No) Blocking List *#3333*#

Init, Flags, Sim Lock *#3377*#

Resetta la (No) Blocking List *#3353*#

Mostra il Security Code *#7489*#

Philips FIZZ

IMEI *#06#

informazioni sul telefono *#8377*#

"Version : 0916 - EEPROM : 00000000-00 - TDA : 1941 - KISS : 0502"

Alcuni telefoni, probabilmente quelli col SIM lock attivato, mostrano la scritta SIM-LCK alla fine della stringa.

security code *#1234*# (1234 è quello di default...)

"Security code : XXXXX"

Service Code *#5644*#

"Version : 09162205 - EEPROM : 0000000-00 - TDA : 1941 - KISS : 0502"

Philips SPARK / GENIE

IMEI *#06#

#2254# : Statusregister: C, BS, RR, MMI, CREAT.

#2255# : attiva e disattiva "DEBUG CALL"-Mode; quando attivato, chiama un numero occupato e il telefono mostrerà delle stringhe esadecimali.

#2558# : Il tempo in ore minuti e secondi in cuisei stato connesso alla rete.

#2562# : IUl telefono si riconnette alla rete

#2565# : warmstart ?

#3333# : (NO) BLOCKING - list (15 oggetti)

#2377# : "BEER": non chiaro. A volte il telefono aspetta un po' e poi si ricollega alla rete, a volte si resetta.

#3377# : Init, Flags, SIM LCK

#3353# : resettta la (NO) BLOCKING - list

#7378# : Name, Length, SIM phase

#7489# : SECURITY CODE

#7693# : attiva e disattiva lo SLEEP MODE (se disattivato la batteria scendera!)

#7787# : SPURIOUS INTERRUPT

#7948# : SWITCH OFF: non chiaro; sembra un timer

#8463# : Informazioni sullo SLLEP MODE: Wake, Sleep Req., Sleep

Philips Pinouts (Fizz e Spark)

1

GROUND

2

GROUND

3

HANDS FREE ON/OFF

4

MUTE

5

TX

6

RX

7

RTS

8

REPROGRAMMING

9

ON HOOK CHARGER (APPROX 13V? TO 14V)

10

AUX MIC

11

AUX SPEAKER

12

GROUND

13

+VCC for Car Charger

+VCC for Car Charger

Tutti i GSM Philips antecedenti il Philip's Fizz sono stati prodotti in cooperazione con la Nokia.

Sezione 5: Storia e Varie

5.1 Non solo scatole blu

Di M.F. Tratto da Decoder

Capita sempre più spesso, sfogliando riviste più o meno specializzate o anche normalissimi

quotidiani, di imbattersi in episodi di pirateria telefonica (utilizzo di determinati servizi eludendo il relativo addebito).

Citando Stephen King, si può dire che tali eventi costituiscono l'inseparabile "metà oscura" della telefonia. Diventa più complicato distinguere in essi ciò che realmente può essere chiamato

"phreaking" e ciò che risulta essere un banalissimo reato; la differenza esiste ed è sostanziale: il phreaker è un esperto di telecomunicazioni che ricerca e utilizza metodi per evitare la tassazione della chiamata, una cosa ben diversa dal furto di un apparecchio cellulare o dallo scasso di un telefono pubblico con trapano e scalpello.

Definito il termine, rimane da chiedersi se in Italia esistano davvero gruppi di phreaker o se nella migliore delle ipotesi esistano solo lamer che si occupano unicamente di utilizzare informazioni provenienti dall'estero, e di cui conoscono solo in parte il significato tecnico. (Il termine "lamer" nel modo informatico indica un incapace che sfrutta passivamente prodotti o metodi elaborati da altri).

Smettiamola quindi per un attimo di pensare agli abili phreaker nordeuropei, americani o australiani ed esaminiamo la situazione del nostro paese.

Chi si serve delle sue conoscenze in campo informatico-telematico per inserirsi in sistemi riservati di scambio dati e acquisire particolari info o privilegi (studiando e bypassando i metodi di protezione adottati) è un hacker; requisito essenziale per un hacker è il possesso di un modem. Hacking e phreaking sono strettamente legati: è utile collegarsi a un sistema senza pagare la telefonata, specie se intercontinentale, e nello stesso tempo lo studio delle caratteristiche di una rete telematica può portare a nuovi metodi di chiamata senza addebito.

Un BBS (banca dati) gestito da un privato o da un gruppo rimane inoltre il miglior mezzo per lo scambio di informazioni, ancora meglio se si tratta di più BBS collegati in rete.

Il Piano Regolatore Telefonico Nazionale (P.R.T.N.) definisce i ruoli delle Aziende che formano il gruppo STET, assegnando a SIP il compito di gestire i rapporti con il singolo utente.

L'inerzia da parte della società nell'accettare la libera diffusione di apparati modem, nei primi anni Ottanta, impedì per lungo tempo l'esplosione del fenomeno banche dati private, al contrario di quanto avveniva all'estero nello stesso periodo; in effetti, da questo punto di vista il nostro paese rimase decisamente arretrato.

In quegli anni erano cominciati in Italia gli esperimenti per la realizzazione di una rete nazionale di interscambio dati sull'onda del successo del network inglese PSS. Tuttavia, gli alti costi di

abbonamento/traffico e la pretesa da parte di SIP di censire ogni modem privato autorizzando solo l'uso di apparati "omologati" limitarono l'utilizzo di questa rete, che fu chiamata Itapac, a pochi privilegiati. In realtà le periferiche "omologate" erano sì prodotti di buona qualità, ma assolutamente uguali a quelli venduti in altri Paesi a 1/3 del prezzo italiano (a quanto pare SIP riuscì a guadagnarci qualcosa, visto che

lo stesso giochetto fu successivamente applicato a cordless, FAX e telefoni cellulari. Attualmente vale solo per questi ultimi).

La diffusione dei compatibili IBM e dei portatili con modem incorporato introdusse l'era dello scambio dati tra utenti in Italia, ma fu il Commodore 64 il vero simbolo informatico della prima metà degli anni Ottanta. Furono importati accoppiatori acustici e modem diretti realizzati per questo computer, e si cominciò a parlare di banche dati, anche se la velocità di trasferimento ammessa dal protocollo CCITT V22 non era molto alta (circa 130 caratteri alfabetici per secondo come punta massima).

L'incognita della mancata omologazione dei suddetti modem restò tale ancora per qualche anno, ma i provvedimenti della compagnia telefonica contro questo tipo di abusi da parte dell'utente furono pochissimi, e tutti giustificati da poco plausibili dichiarazioni di danni arrecati alle linee a causa di manipolazioni non autorizzate.

Nello stesso periodo SIP cominciò a sentire la necessità dei una rete di servizi più vicina all'utente, copiò i modelli europei e partorì una mostruosa creatura: il Videotel (VDT).

Per ridurre le raffiche di spurie, effetti delle interferenze elettromagnetiche sulle linee, fu utilizzato il protocollo CCITT V23-1200/75 BPS, tuttora in uso, associato a sistemi di correzione dei dati

trasmessi. Questa scelta impose l'acquisto di un modem che prevedesse tale non comunissimo

formato, oppure l'impiego del terminalino fornito da SIP stessa.

Videotel fu un prodotto sciagurato: non incontrò il previsto favore popolare, e i gestori fecero di tutto per promuoverlo trascurandone il difetto principale: i costi di collegamento oltre ogni razionale proporzione, Come primo errore, riempirono il sistema di account intestati a utenti inesistenti, che subito finirono nelle mani di decine di abusivi. Se la diffusione di tali codici di accesso fu in un certo senso calcolata, per motivi pubblicitari, non fu previsto l'effetto collaterale: con una buona quantità di password facilmente a

disposizione, gli hacker dedussero al volo il peraltro elementare algoritmo che le generava.

Commodore commercializzò un piccolo modem per connettere C64 a VDT e successivamente

Philips ideò un interfaccia che trasformava il televisore di casa in un terminalino: la caccia alla password Videotel divenne uno sport nazionale.

Sul piano del phreaking, il canale della pirateria software (da sempre strettamente legato agli abusi telefonici) continuò a regalare aneddoti e informazioni, specialmente di origine americana o

nordeuropea; in Italia tuttavia mancavano le condizioni per poterle utilizzare.

Unica eccezione la black box, sperimentata anche nel nostro paese diverso tempo prima, che fu

riesumata: si trattava di un semplice gruppo di componenti elettronici (talvolta un solo resistore) che compensando la variazione di un parametro fisico della linea impediva alla centrale dell'utente di rilevare che egli aveva appena risposto a una chiamata. In tal modo, il chiamante non riceveva addebito per quella comunicazione.

Nonostante la diffusione in alcuni paesi del nostro continente, non si può parlare di un fenomeno

"black box" in Italia. Il metodo, molto vecchio, non ebbe mai successo, stroncato anche da centrali urbane di più recente concezione in grado di rilevare ed escludere questo tipo di anomalie.

Nella seconda metà degli anni Ottanta Italcable presentò nuovi servizi, primi tra tutti i numeri verdi internazionali estesi a più Paesi. Questo permise ai phreaker di importare una tecnica divenuta famosa all'estero circa un decennio prima con il nome di blue box (il primo modello individuato era appunto alloggiato in una scatola blu), le cui origini sono tuttora controverse:

qualcuno ne attribuisce la paternità agli stessi progettisti o tecnici delle linee internazionali; per certo, protagonisti storici dell'informatica si dedicarono al perfezionamento di tale piccolo apparato. Questo dispositivo, reale o simulato dal software, grazie all'imitazione di alcune frequenze di dialogo tra centrali telefoniche di un certo tipo, permetteva di indirizzare ad altro utente una chiamata

originariamente instradata su numero verde, evitando così l'addebito.

Semplice e raffinata, la blue box non produceva un reale danno economico ai concessionari delle linee, ma era per contro un'entità troppo conosciuta.

Dalle compagnie telefoniche stesse innanzitutto, e poi, se non altro come "leggenda", dai ragazzi di mezzo pianeta.

Degli oltre venti tipi di box realizzati negli USA, non si hanno notizie di impieghi rilevanti, nel nostro paese, per modelli diversi dai due citati: casi isolati di interconnnessione abusiva di due linee o tentativi di vandalismo telefonico rientrerebbero nella categoria "boxes" ma furono fatti più unici che rari.

A partire dal 1986 iniziò la proliferazione incontrollata, nell'ambiente Videotel, dei servizi di messaggeria, o chat (centoquaranta in meno di cinque anni); la prima messaggeria internazionale, accessibile in seguito all'interconnessione Videotel-Minitel divenne uno dei punti di incontro degli hacker di quel periodo. La qualità e la diffusione dei modem migliorarono di molto, intorno al 1987 si potevano acquistare discreti prodotti e installarli senza difficoltà nè problemi con la compagnia telefonica.

Itapac era già conosciuta nelle università perché la rete telematica accademica (oggi nota come Internet, è un network di reti) era collegata con essa; il solito Videotel inoltre si appoggiava (e si appoggia) a Itapac per raggiungere i servizi. Gli hacker dunque iniziarono a usare tale sistema di scambio dati per raggiungere nuovi ambienti telematici italiani ed esteri.

Alcuni codici di accesso usati intorno al 1988 divennero famosi. Con la diffusione di Amiga la pirateria del software, primo e spesso unico mezzo di importazione e diffusione, fece un salto di qualità; il modem divenne una periferica comune, utilizzata per il prelievo delle ultime novità per lo stesso Amiga o per MS-DOS dalle numerose banche dati che andavano nascendo in quel periodo.

Nuovi metodi di correzione errori eliminarono l'incubo delle spurie.

L'azienda statunitense US Robotics sviluppò un protocollo non omologato dal CCITT per

trasmissioni ad alta velocità; questi modems, largamente utilizzati anche nel nostro paese, risolsero il problema della lentezza di trasferimento anche se il costo dell'apparato rimase alto fino alla diffusione di modem concorrenti, avvenuta molto più tardi grazie all'introduzione dello standard CCITT V32bis.

Siamo sempre nella seconda metà degli anni Ottanta: il nuovo algoritmo elaborato per la

generazione di password Videotel fece in breve la fine del suo predecessore. I contrasti per motivi economici tra i fornitori di informazione di Videotel e la compagnia telefonica divennero pesanti, SIP

stessa decise di ridurre la sua partecipazione alla gestione del servizio (attualmente si occupa solo del sistema di sicurezza e dei rapporti diretti con l'utente).

L'accesso a Itapac cessò di essere un fenomeno d'elite nel settembre 1989, quando alcuni codici superarono le frontiere del ristretto mondo degli hacker e iniziarono a essere utilizzati da utenti più

"novellini". Itapac permetteva il collegamento a banche dati americane anche al di fuori della rete stessa grazie a particolari indirizzi detti outdialers; fu l'aspetto più interesssante del network in quegli anni, dopo i servizi di messaggeria. Speciali outdialer inoltre potevano raggiungere gratuitamente una banca dati in qualsiasi parte del mondo, unico difetto la lentezza di Itapac e il fatto che la chiamata avesse origine fisica negli Stati Uniti, con tutti i problemi che potevano derivare da una connessione intercontinentale a bassa velocità.

Ma Itapac era utilizzabile soltanto da determinate città, concentrate nel Nord del paese; nel 1990 SIP

introdusse il numero verde nazionale 1421 che consentì l'accesso alla rete con precise limitazioni (reverse charging) da tutt'Italia, anche se ci volle molto tempo per il completamento del servizio.

Nel settembre 1990, in occasione di SMAU, un periodico pubblicò a scopo dimostrativo un codice di accesso a Itapac 1421 valido senza restrizioni su tutto il territorio nazionale; questo fu l'episodio più famoso nella storia della rete e interessò centinaia di proprietari di modem:

quando tale password (5GFvdD) fu disattivata, nel gennaio1991, l'accesso al network era divenuto un vizio ed esplose il bisogno di altri codici validi. L'implementazione del collegamento

"countrydirect" intanto, aveva apero nuove frontiere per il phreaking, legate specialmente all'importazione software. Si trattava di numeri gratuiti internazionali che permettevano di usare servizi e sistemi di addebito di compagnie straniere, ad esempio le carte di credito telefoniche statunitensi i cui numeri, da anni, erano oggetto di collezione e scambio tra i pirati telematici. Con un pò di lingua inglese e un numero di carta USA valido, la chiamata gratuita negli States fu possibile per tutti; per raggiungere altre nazioni serviva solo qualche codice in più, quello dei PBX.

Bridges, loops, conferences, e altri gadget tipici delle reti nordamericane, furono alla portata dei phreaker italiani; fu ad esempio possibile chiamare contemporaneanente 8, 10, 15 persone disperse in varie parti del mondo. Videotel rese disponibili simpatici servizi di addebito su password per l'acquisto di piccoli oggetti, e i phreaker trascorsero l'allegro periodo dei mondiali di calcio inviandosi a spese di terzi orchidee e adesivi personalizzati.

Difetti nel software delle centrali elettroniche fecero nascere in quegli anni strane voci su possibili nuove

tecniche di phreaking, ma non vi furono novità rilevanti.

Verso la fine del 1990, iniziarono a essere create in banche dati private aree di hacking/phreaking degne di questo nome; l'esperimento di aprire spazi simili all'interno di un network di BBS sarà in seguito tentato da due reti nazionali, EuroNet e FidoNet; in entrambi i casi la smisurata paranoia di alcuni pseudo-responsabili condurrà all'aborto del progetto, seriamente ripreso solo dalla neonata CyberNet nell'aprile 1993. Nel dicembre 1990, due novità: il primo PBX su numero verde 1678 e il primo outdialer in grado di chiamare gratuitamente banche dati in ogni parte del mondo a partire da Milano.

Venne l'estate '91, e una serie di inchieste giudiziarie assestò un duro colpo alle truffe che i fornitori di informazione di Videotel perpetravano da tempo di danni di SIP. Questi episodi, naturalmente, non ebbero nulla a che vedere con il fenomeno dell'hacking ma rivelarono una volta per tutte le lacune del sistema.

Le possibilità del reverse charging (Itapac 1421) furono adeguatamente esplorate, si scoprì così che dopo tutto non era affatto necessario possedere un codice di accesso per penetrare nella rete.

Sempre tramite Itapac, fu trovato il modo di inviare FAX ed espressi a qualsiasi destinatario, ovviamente senza spendere nulla (1991/92). Per quanto riguarda i posti telefonici pubblici, è

obbligatorio citare l'applicazione di nastro isolante sulla scheda magnetica a scalare, notissimo esempio dell'inaffidabilità di quella generazione di lettori Urmet. Di circa tre anni prima, l'altrettanto nota abitudine di resettare il telefono pubblico inserendo una scheda piegata in due nella fessura superiore dell'apparecchio, conseguenza di un errata progettazione di quella macchina; altri metodi più recenti hanno invece a che fare con le linee elettroniche. Il boom della telefonia cellulare attirò ovviamente l'attenzione dei phreaker, non senza il supporto di tecnici e rivenditori alla ricerca di un mezzo per arrotondare gli introiti. Poche EPROM riprogrammate per i nuovi 900MHz, un interesse maggiore per la precedente rete veicolare 450MHz, ormai abbandonata a se stessa e molto più

sicura dal punto di vista del violatore di sistemi. In seguito, SIP riferirà ogni episodio di frode (ovviamente scoperta) esclusivamente agli adorati telefonini 900MHz: come il grande Oscar Wilde insegna, ogni scusa è buona per parlare del prodotto. Specie quando il prodotto, sempre grazie all'anacronistico monopolio che caratterizza il mercato italiano, ha un costo scandaloso aggravato da un'insensata tassa di lusso. (Piccola nota: se credete che la cosa non vi tocchi, sappiate che sono ben 9842, secondo il dossier Pagani in risposta all'interrogazione parlamentare dell'On. Gasparri, i portatili le cui bollette sono interamente spesate con denaro pubblico: l'apoteosi dello spreco!).

La più infelice creatura dei primi anni Novanta rimane comunque la carta di credito SIP, altrimenti nota come "carta infinita": comoda e pratica ma non dotata di alcuna forma di protezione, a eccezione di tre codici (il terzo è il checksum) facilmente calcolabili e un controllo tramite operatore bypassabile senza troppo sforzo.

Nel settembre 1991 la blue box sfuggì al controllo di pochi gruppi telematici (anche per interessi personali di alcuni membri) e divenne una tecnica paurosamente diffusa; di conseguenza, i veri phreaker cominciarono a disprezzare il metodo in questione o quantomeno a intrudurre varianti

personali che riducessero il rischio connesso a un fenomeno di massa. Ciò non impedì a quest'entità di dominare l'intero 1992. La notorietà della scatola blu fu la prefazione al suo certificato di morte.

Modifiche più o meno rilevanti introdotte a livello internazionale nei sistemi di segnalazione, dietro sicura pressione delle più grandi aziende di telecomunicazioni, cancellarono lentamente le possibilità di un suo utilizzo. All'inizio del 1993, delle procedure più classiche di blue boxing, non esisteranno superstiti di effettiva utilità pratica.

Sempre nel 1992, l'automatizzazione di diversi servizi USA raggiungibili dall'Italia con un semplice apparecchio multifrequenza eliminò la necessità di un dialogo diretto con gli operatori stranieri.

Insistenti voci su un pericolo di concorrenza (termine sconosciuto per legge alla compagnia

telefonica italiana) cambiarono l'atteggiamento dei responsabili di Itapac: vagamente migliorato il servizio, nacque la necessità di dimostrare la capacità di acchiappare almeno un utente irregolare; le vittime furono piccoli appassionati di messaggerie completamente estranei al vero

hacking/phreaking, tuttavia lo scopo dimostrativo fu raggiunto e puntualmente gonfiato dalla stampa con formulazione di tesi deliranti.

Notevolmente migliorato (almeno sulla carta) anche il sistema di accesso a VDT: addebito diretto al chiamante, soluzione palesemente copiata all'estero e in fondo una sorta di "uovo di Colombo".

(Nota: il sistema è ancora in fase sperimentale alla data odierna).

Nello stesso anno vedranno la luce gli apparecchi telefonici pubblici "cards only", doverosi sostituti (in nome della sicurezza) degli ancora giovanissimi ma malati predecessori.

E il 1993? Si attende l'implementazione di un certo numero di nuovi servizi e il naturale studio dei medesimi da parte degli hacker/phreaker, si attendono gli effetti sull'ambiente telematico

dell'ulteriore, notevole crescita degli utilizzatori di modem. Nulla di particolamente stimolante?

Forse... ma nessuno dei grandi eventi nella storia underground della telematica fu mai preventivato, e questo è evidente. Esiste una certa curiosità, inoltre, anche per il crescente interesse del pubblico sull'argomento; uno dei motivi che mi hanno spinto a scrivere questo articolo, in nome della

controinformazione, è che ero stufo di leggere i soliti commenti da parte di cosiddetti esperti del ramo: gente che oggi sputa sentenze e solo ieri progettava sistemi tra i più hackerati del globo.

I violatori di sistemi hanno sempre riconosciuto l'abilità dei propri antagonisti e lo stesso

hacking/phreaking, che esiste in nome del libero diritto all'informazione, si può considerare una sorta di sfida tra esperti di telecomunicazioni. In questo senso, e solo in questo, sono felice di constatare che rimangono ancora molte porte da aprire.

5.2 La natura Giuridica del Phone Phreaking

di Andrea Monti

Sul fatto che l'uso di mezzi o apparecchiature di varia complessità e natura diretti ad evitare l'addebito sulla propria bolletta sia illegittimo non c'è alcun dubbio; qualcuno ne sorge, invece, quando ci si ponga il problema di individuare, in concreto, quale reato sia stato commesso.

La questione è tutt'altro che priva di interesse pratico dal momento che nel nostro ordinamento penale, come è noto, nessuno può essere punito per un fatto che al tempo in cui è stato commesso non era previsto dalla legge come reato; ciò vuol dire, in altri termini, che se non è possibile ricondurre l'impiego delle "Blue-Box" (o di apparecchiature o software aventi analoga funzione) ad una norma penale vigente non viene commesso nessun reato (salva, ovviamente, la risarcibilità del danno in sede civile).

Siccome non esiste nessuna legge che vieta esplicitamente l'impiego di questi apparecchi sarebbe, allora, immediato dedurre che usare le "Blue-Box" sia quantomeno non-illegale, ma le cose non sono così semplici.

Il problema di qualificare giuridicamente le interferenze abusive sulla rete telefonica è noto da parecchio tempo: già nel 1977, infatti, la Corte di Cassazione ebbe ad occuparsi di un caso del genere pronunciando una sentenza della quale si riporta qui di seguito la massima:

"La captazione fraudolenta di un servizio o di una prestazione (nella specie, collegamento abusivo di un apparecchio telefonico con la cabina di zona della SIP mediante allacciamento della linea di servizio riservata alla società) può astrattamente integrare in concorso con degli altri elementi all'uopo richiesti dalla legge, e - segnatamente dell'ingiusto profitto e del danno patrimoniale - le ipotesi del delitto di truffa.

Non può invece ravvisarsi nel fatto il reato di furto dal momento che manca la cosa mobile (o

l'energia ad essa equiparata) sulla quale deve cadere, ai fini della configurabilità dell'ipotesi di cui all'art.624 c.p., l'azione dell'impossessamento. Infatti le utenze telefoniche private - gestite in regime di concessione ad una società privata, quale la SIP, anche se con partecipazione di capitale

pubblico - realizzano una ipotesi di somministrazione di un servizio, e non di una energia, benchè questa sia essenziale al servizio stesso (le vibrazioni acustiche sono trasformate, nella telefonia, in vibrazioni elettriche, ma oggetto della utenza è il servizio in sé, e non già l'energia che lo rende possibile).

In difetto del delitto di truffa, può configurarsi nel fatto la specifica ipotesi di reato prevista dal d.p.r.

29/03/73 n. 156 che dichiara perseguibile, ai sensi dell'art.3 c.p., chiunque esplichi attività che rechino danno ai servizi postali e di telecomunicazione od alle opere ed oggetti ad essi inerenti (art.23)." - Cass.Pen. Sez.I, 21-12-77.

In estrema sintesi i principi enunciati da questa sentenza sono i seguenti:

1) La captazione fraudolenta del servizio telefonico non è furto perchè manca la "cosa mobile altrui"

che dovrebbe venir sottratta a chi la detiene, secondo il testo dell'art.624 c.p.

2) Viceversa potrebbe configurarsi la truffa, ma per il verificarsi di questa ipotesi sarebbe necessario provare di aver ingannato qualcuno per ottenere l'ingiusto profitto, così infatti recita l'art.640 c.p. :

"Chiunque, con artifizi e raggiri, inducendo taluno in errore, procura a sè o ad altri un ingiusto profitto con altrui danno, è punito ....".

In altri termini, ciò che dovrebbe essere punito, in questo caso, non è il phreaking fine a se stesso quanto piuttosto il suo impiego al fine di compiere gli artifizi e raggiri menzionati dal codice penale; che poi questo sia difficile da provare è un altro discorso.

3) Se non è possibile configurare la truffa allora potrebbe essere applicabile l'art. 23 d.p.r. 29/03/73

n. 156.

E' ragionevole sostenere che anche l'impiego delle "Blue-Box" rientri fra le ipotesi contemplate dalla sentenza in questione e che, quindi, sia qualificabile come "fraudolenta captazione di servizi o prestazione", anche se, ad oggi, non sembrano essere stati registrati precedenti giudiziari specifici.

L'unica soluzione per risolvere definitivamente il problema era quella di prevedere una specifica ipotesi di reato che individuasse esattamente non solo cosa, ma anche e soprattutto, come punire.

L'occasione (persa) poteva giungere dalla legge che ha inserito nel codice penale i c.d. "Computer crimes".

Fra i reati introdotti dalla L.547/93 il candidato a risolvere la questione che ha aperto il presente scritto avrebbe potuto essere quello previsto dall'art.640ter (frode informatica).

Il testo dell'articolo in questione così recita:

"Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sè o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni.

La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se se ricorre una delle circostanze previste da numero 1) del secondo comma dell'art.640, ovvero se il fatto è commesso con l'abuso della qualità di operatore del sistema .

Il delitto è punibile a querela della persona offesa salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante."

Una prima superficiale lettura dell'articolo non aiuta a chiarire le cose.

L'articolo 640 ter c.p., infatti, si riferisce esclusivamente ai sistemi informatici e telematici ma non prende affatto in considerazione il problema del phreaking.

Del resto è la legge stessa che differenzia nettamente l'ambito informatico-telematico da quello telefonico come nell'art.623 bis c.p. dove le forme di comunicazione vengono distinte in telefoniche, telegrafiche, informatiche e telematiche, o in materia di intercettazioni telefoniche dove sussiste la medesima

classificazione.

Nella stessa direzione si muove la dottrina che definisce "sistema informatico" "... più elaboratori elettronici collegati fra loro per scambiare dati" (AA.VV., Profili penali dell'informatica, Giuffrè 1994

p.148), se il collegamento avviene per mezzo di cavi telefonici, onde guidate ecc. allora il sistema diventa "telematico" (ibidem).

Sarebbe ovvio concludere che siccome il phreaking non riguarda i "sistemi" menzionati dalla legge ma

solo dei centralini telefonici, esso non dovrebbe rientrare nell'ambito di vigenza dell'art.640ter.

A ben vedere, tuttavia, molte delle tecniche impiegate per procurarsi la disponibilità delle linee telefoniche hanno come bersaglio il software che gestisce la centrale telefonica, risultando idonee ad alterare il funzionamento del sistema così come previsto dalla norma in oggetto.

In conclusione, quindi, bisognerebbe distinguere il metodo di phreaking impiegato: l'uso di

apparecchi o

sistemi che non interagiscono direttamente con un computer probabilmente non rientra nell'ambito di validità dell'art. 640ter, e allora valgono le considerazioni svolte in precedenza.

Il ricorso a sistemi che coinvolgono direttamente un elaboratore dovrebbe essere invece punibile ai sensi del predetto articolo, a nulla rilevando, peraltro, che il "bersaglio" del phreaker sia oltre confine o oltre oceano.

5.3 Mentor’s Last Words

The Hacker’s Manifesto

Ne e' stato arrestato un altro oggi, e' su tutti i giornali.

"Ragazzo arrestato per crimine informatico", "Hacker arrestato dopo essersi infiltrato in una banca"...

Dannati ragazzini. Sono tutti uguali. Ma avete mai, con la vostra psicologia da due soldi e il vostro tecno-cervello da anni 50, guardato dietro agli occhi del Hacker? Non vi siete mai chiesti cosa abbia fatto nascere la sua passione? Quale forza lo abbia creato, cosa puo' averlo forgiato? Io sono un hacker, entrate nel mio mondo...

Il mio e' un mondo che inizia con la scuola... Sono piu' sveglio di molti altri ragazzi, quello che ci insegnano mi annoia...

Dannato sottosviluppato. Sono tutti uguali. Io sono alle Junior High, o alla High School. Ho ascoltato gli insegnanti spiegare per quindici volte come ridurre una frazione. L'ho capito. "No, Ms. Smith, io non mostro il mio lavoro. E' tutto nella mia testa..."

Dannato bambino. Probabilmente lo ha copiato. Sono tutti uguali. Ho fatto una scoperta oggi. Ho trovato un computer. Aspetta un momento, questo e' incredibile! Fa esattamente quello che voglio.

Se commetto un errore, e' perche' io ho sbagliato, non perche' io non gli piaccio... O perche' si senta minacciato da me... O perche' pensi che io sia un coglione... O perche' non gli piace insegnare e vorrebbe essere da un'altra parte... Dannato bambino. Tutto quello che fa e' giocare. Sono tutti uguali.

Poi e' successa una cosa...una porta si e' aperta su un mondo...correndo attraverso le linee

telefoniche come l'eroina nelle vene del tossicomane, un impulso elettronico e' stato spedito, un rifugio dagli incompetenti di ogni giorno e' stato trovato, una tastiera e' stata scoperta.

"Questo e'...questo e' il luogo a cui appartengo..." Io conosco tutti qui...non ci siamo mai incontrati, non abbiamo mai parlato faccia a faccia, non ho mai ascoltato le loro voci...pero' conosco tutti.

Dannato bambino. Si e' allacciato nuovamente alla linea telefonica. Sono tutti uguali. Ci potete scommettere il culo che siamo tutti uguali...noi siamo stati nutriti con cibo da bambini alla scuola mentre bramavamo una bistecca... i pezzi di cibo che ci avete dato erano gia stati masticati e senza sapore. Noi siamo stati dominati da sadici o ignorati dagli indifferenti. I pochi che avevano qualcosa da insegnarci trovavano in noi volenterosi allievi, ma queste persone sono come gocce d'acqua nel deserto.

Ora e' questo il nostro mondo...il mondo dell'elettrone e dello switch, la bellezza del baud. Noi facciamo uso di un servizio gia esistente che non costerebbe nulla se non fosse controllato da approfittatori ingordi, e voi ci chiamate criminali. Noi esploriamo...e ci chiamate criminali. Noi cerchiamo conoscenza...e ci chiamate criminali. Noi esistiamo senza colore di pelle, nazionalita', credi religiosi e ci chiamate criminali. Voi costruite bombe atomiche, finanziate guerre, uccidete, ingannate e mentite e cercate di farci credere che lo fate per il nostro bene, e poi siamo noi i criminali.

Si, io sono un criminale. Il mio crimine e' la mia curiosita'. Il mio crimine e' quello che i giurati pensano e sanno non quello che guardano. Il mio crimine e' quello di scovare qualche vostro

segreto, qualcosa che non vi fara' mai dimenticare il mio nome.

Io sono un hacker e questo e' il mio manifesto. Potete anche fermare me, ma non potete fermarci tutti...dopo tutto, siamo tutti uguali.

The Mentor

5.4 Lo sfogo di un Phreaker

Siete tutti dei lamer, qui non esistono veri phreakers. Siete solo povera gente che crede che scrivere in un gruppo come questo (per fortuna libero, e ringrazio chi l'ha reso tale) significhi essere gente

"del giro".

Ma VOI, cosa avete mai fatto di realmente phreak? E soprattutto, cosa sareste REALMENTE

disposti a fare? Avete mai provato il brivido freddo che scorre lungo la schiena del phreaker che tenta una tecnica in una cabina telefonica, sperando che l'ultimo passante che l'ha guardato non chiami gli sbirri? No? Allora PRIMA studiate elettronica, telefonia, informatica e cercate di conoscere della gente IN GAMBA. Imparate le tecniche con umiltà.

Provatele seriamente. Solo allora forse potrete dire di essere del giro. Voi non sapete neanche cosa vuol dire phreaker. A meno che - e ne sarei contento - queso "news" non sia vuoto perchè la gente Sta studiando e non ha tempo da perdere. E non perchè nessuno sa cosa dire. Pensateci. Non

pensate a chi possa essere io. Pensate a cosa potreste diventare VOI se non foste qui a volere tutto pronto ma

se foste veramente disposti a darvi da fare.

Appendice 1: Leggende Metropolitane

Di CDP

Da quando ho iniziato a dedicarmi al phreaking, ho notato che giravano voci strane e tecniche

apparentemente assurde che poi invece si verificavano… assurde!

Non so chi ha avuto l'idea malsana di metterle in giro, ma alcune (c'è gente che le ha perfino provate…) sono proprio comiche, anche se denotano una notevole fantasia associata ad una

completa inesperienza.

Mitica è la storiella che io ho sentito parecchie volte dei numerini che andavano digitati dopo il numero da chiamare per non pagare, il tutto da un telefono cellulare. Chiaramente conoscendo il funzionamento del sistema telefonico si capisce che tali numeri venivano completamente ignorati.

"From: "Nicola " < xxxxxxxxx@tin.it >

To: < spaghettiphreak@hotmail.com >

Subject: gratis dal cellulare?

Date: Tue, 28 Apr 1998 02:36:45 +0200

Non è vera la storia dei numerini segreti alla fine del

numero da chiamare dal cellulare...

Avevo una media di L. 100.000 a bolletta....dopo quei

numerini...che io ho usato spesso (perchè garantiti

sicuri) ho ricevuto L. 1.200.000 di

bolletta....convinti??????? ciao

Nike"

Vedete anche voi che non ci sono dubbi…. Questa storia è assimilabile a quel a del tizio che fa l'incidente con la moto, si rialza, ma non appena si toglie il casco gli si apre in due la testa! Mio cuggino docet…

E cosa dire poi degli assurdi metodi per ricaricare le schede telefoniche telecom? Passi il metodo dello scotch che in effetti era valido sul a prima generazione dei lettori Urmet (primi anni '90), ma gli altri…

La tessera nel sale, lo schermo della TV a b/n (perché emettono più radiazioni…), il registratore del Commodore 64 o addirittura il forno a microonde e l'accendino!!

La gente ci ha provato lo stesso, però…

"La carta telefonica dentro il sale per qualche giorno o sul televisore b/n acceso da qualche ore per ricaricarla sono delle belle leggende metropolitane ...io (scemo!) ci ho pure provato

.... NON FUNZIONA!!!

Non funziona con le chede scariche e non funziona con quelle che hanno ancora dentro qualche lira.

E' probabile invece che il televisore smagnetizzi quelle cariche... questo si!!!

(E' possibile che le interferenze magnetiche del televisore modifichino l'importo della scheda a vostro favore: la probabilita' di riuscita puo' essere paragonata a quella di far centro con un bottone in una giornata ventosa dentro un bicchiere posto a dieci metri di distanza.)

Lo scotch sulla banda per non far modificare l'importo dal lettore: che cazzata!!! se il lettore non e' in grado di scrivere il codice ovviamente non puo' nenche essere in gradi di leggerlo no!!!!

Master"

Queste e tante altre sono le leggende metropolitane che circondano il mondo del Phreaking.. e altre ne verranno fuori non appena nuove frontiere saranno superate, specie quelle della fantasia.